Privacy-Handbuch

Spurenarm Surfen mit Mozilla Firefox,
E-Mails verschlüsseln mit Thunderbird,
Anonymisierungsdienste nutzen
und Daten verschlüsseln
für WINDOWS + Linux

1. April 2017

Wir sind die Vielen,
wir könnten einen Beat stampfen,
der jede Macht pulverisieren wird.

Inhaltsverzeichnis

1 Scroogled **8**

2 Angriffe auf die Privatsphäre **21**
2.1 Big Data - Kunde ist der, der bezahlt . . . 22
2.1.1 Google . . . 22
2.1.2 Weitere Datenhändler . . . 30
2.2 Techniken der Datensammler . . . 32
2.3 Tendenzen auf dem Gebiet des Tracking . . . 38
2.4 Crypto War 3.0 . . . 42
2.5 Fake News Debatte . . . 44
2.6 Geotagging . . . 47
2.7 Kommunikationsanalyse . . . 50
2.8 Überwachungen im Internet . . . 53
2.9 Terrorismus und Ausbau der Überwachung . . . 61
2.10 NSA & Co. . . . 64
2.11 Rechtsstaatliche Grundlagen . . . 65
2.12 Bundesamt für Verfassungsschutz auflösen . . . 67
2.13 Ich habe doch nichts zu verbergen . . . 73

3 Digitales Aikido **77**
3.1 Nachdenken . . . 77
3.2 Ein Beispiel . . . 81
3.3 Schattenseiten der Anonymität . . . 83
3.4 Wirkungsvoller Einsatz von Kryptografie . . . 84

4 Spurenarm Surfen **87**
4.1 Auswahl des Webbrowsers . . . 88
4.2 Datensparsame Suchmaschinen . . . 90
4.3 Cookies . . . 96
4.4 EverCookies . . . 99
4.5 JavaScript . . . 102
4.5.1 NoScript für Mozilla Firefox . . . 103
4.6 iFrames . . . 107
4.7 Werbung, HTML-Wanzen und Social Media . . . 107
4.7.1 Tracking-Filter für Firefox . . . 109
4.7.2 Tracking Protection in Firefox . . . 110
4.7.3 uBlock Origin für Firefox . . . 110
4.7.4 Adblock Plus für Firefox . . . 111

4.7.5 Werbung auf der NewTab Page . . . 113
4.8 History Sniffing . . . 115
4.9 Browsercache und Chronik . . . 116
4.10 Referer . . . 118
4.11 Risiko Plugins . . . 119
4.11.1 PDF Reader Plugins . . . 119
4.11.2 Java-Applets . . . 120
4.11.3 Flash-Applets und Flash-Videos . . . 122
4.11.4 Weitere Anwendungen . . . 124
4.11.5 H.264 Plug-in und Adobe Primetime deaktivieren . . . 124
4.12 HTTPS-Verschlüsselung nutzen . . . 125
4.13 Vertrauenswürdigkeit von HTTPS . . . 127
4.13.1 Verbesserung der Vertrauenswürdigkeit von HTTPS . . . 128
4.13.2 Firefox Add-ons . . . 129
4.13.3 SSL-Zertifikate via OCSP validieren . . . 131
4.13.4 Tracking via SSL Session . . . 133
4.13.5 Tracking via HTTP Strict Transport Security (HSTS) . . . 134
4.13.6 SSL/TLS Konfiguration . . . 135
4.14 Starke Passwörter nutzen . . . 137
4.15 Zwei-Faktor-Authentifizierung . . . 139
4.16 Installierte Schriftarten verstecken . . . 142
4.17 HTML5 Canvas Elemente . . . 143
4.18 recource:// URIs blockieren . . . 145
4.19 User-Agent modifizieren für Firefox . . . 146
4.20 Hardware Fingerprinting . . . 148
4.21 Sonstige Maßnahmen . . . 150
4.22 Snakeoil für Firefox (überflüssiges) . . . 154

5 Bezahlen im Netz 156
5.1 Kreditkarten . . . 157
5.2 Bezahlsysteme der Deutschen Bahn . . . 158
5.3 SOFORT Überweisung . . . 158
5.4 Paysafecard, UKash, Pecunix . . . 159
5.5 Anonyme Online-Zahlungen vor dem Aus? . . . 161
5.6 Bargeld . . . 163
5.7 Bitcoin . . . 166
5.7.1 Exchanger / Marktplätze . . . 167
5.7.2 Bitcoin Software . . . 168
5.7.3 Anonymität von Bitcoin . . . 170
5.7.4 Bitcoin anonym nutzen . . . 172

6 E-Mail Kommunikation 174
6.1 E-Mail Provider . . . 174
6.2 Mozilla Thunderbird . . . 178
6.2.1 Account erstellen . . . 178
6.2.2 Sichere Optionen für SSL/TLS-Verschlüsselung . . . 181
6.2.3 Sichere Konfiguration des E-Mail Client . . . 186
6.2.4 Datenverluste vermeiden . . . 189
6.2.5 Wörterbücher installieren . . . 190
6.2.6 User-Agent Kennung modifizieren . . . 190

6.2.7 Spam-Filter aktivieren 192
6.2.8 Spam vermeiden 192
6.2.9 RSS-Feeds 197
6.2.10 Filelink 198
6.3 Private Note 200
6.4 ProtonMail, Tutanota und andere 202

7 E-Mails verschlüsseln 205
7.1 GnuPG und Thunderbird 207
7.1.1 Installation von GnuPG 207
7.1.2 Verbesserte Konfiguration von GnuPG 207
7.1.3 Installation der Enigmail-Erweiterung 208
7.1.4 Schlüsselverwaltung 210
7.1.5 Signieren und Verschlüsseln erstellter E-Mails 212
7.1.6 Adele - der freundliche OpenPGP E-Mail-Roboter 213
7.1.7 Verschlüsselung in Webformularen 215
7.1.8 Browser Add-ons wie Mailevelop 216
7.1.9 GnuPG Smartcard nutzen 216
7.1.10 OpenPGP Keyserver 221
7.1.11 Mailvelope Browser Add-on 224
7.1.12 OpenPGP-Verschlüsselung für Kontaktformulare 226
7.1.13 Web des Vertrauens 228
7.1.14 Schlüssel zurückrufen 231
7.2 S/MIME mit Thunderbird 232
7.2.1 Kostenfreie Certification Authorities 232
7.2.2 Erzeugen eines Zertifikates 233
7.2.3 S/MIME-Krypto-Funktionen aktivieren 234
7.2.4 Zertifikate der Partner und der CA importieren 235
7.2.5 Nachrichten verschlüsseln und signieren 236
7.2.6 Root-Zertifikate importieren 237
7.2.7 Eine eigene Certification Authority 238
7.2.8 Ist S/MIME-Verschlüsselung unsicher? 239
7.3 E-Mail als verschlüsseltes Dokument senden 243
7.4 Eine Bemerkung zum Abschluß 243

8 E-Mail jenseits der Überwachung 245
8.1 Anonyme E-Mail Accounts 245
8.2 Private Messages in Foren nutzen 246
8.3 alt.anonymous.messages 246
8.4 Mixmaster Remailer 246

9 Instant Messaging 254
9.1 Jabber (XMPP) 254
9.2 Jabber/XMPP Client Gajim 260

10 Verschlüsselt telefonieren 265
10.1 Open Secure Telephony Network (OSTN) 266
10.1.1 OSTN-Provider 267
10.2 VoIP-Client Jitsi 268

11 Anonymisierungsdienste **271**
11.1 Warum sollte man diese Dienste nutzen? 271
11.2 Tor Onion Router 274
11.2.1 Security Notes 278
11.2.2 Anonym Surfen mit dem TorBrowserBundle 279
11.2.3 Tor Hidden Services 285
11.2.4 Anonyme E-Mails mit Thunderbird 292
11.2.5 Anonym Bloggen 296
11.2.6 Anonymes Instant-Messaging 297
11.2.7 Anonymes Instant-Messaging mit TorMessenger 298
11.2.8 Pidgin für Linux und Tor Onion Router 301
11.2.9 Gajim (Linux) und Tor Onion Router 303
11.2.10 Anonymes Instant-Messaging mit TorChat 306
11.2.11 Anonymes Instant-Messaging mit Ricochet 308
11.2.12 Dateien anonym tauschen via Tor 309
11.2.13 Tor Bad Exit Nodes 311
11.2.14 Tor Good Exit Nodes 315
11.3 Finger weg von unseriösen Angeboten 317
11.3.1 Tor-Boxen 317
11.3.2 Web-Proxys 317
11.3.3 Free Hide IP 318
11.3.4 ZenMate 318
11.3.5 5socks.net 319
11.3.6 BlackBelt Privacy, Cloakfish und JanusVM 321
11.3.7 Proxy-Listen 322

12 Anonyme Peer-2-Peer Netzwerke **323**
12.1 Invisible Internet Project (I2P) 325
12.1.1 Installation des I2P-Routers 325
12.1.2 Konfiguration des I2P-Router 327
12.1.3 Anonym Surfen mit I2P 329
12.1.4 I2P Mail 1 (Susimail) 331
12.1.5 I2P Mail 2 (Bote) 333
12.1.6 I2P IRC 337
12.1.7 I2P BitTorrent 339
12.2 DSL-Router und Computer vorbereiten 340

13 Daten verschlüsseln **341**
13.1 Konzepte der vorgestellten Tools 342
13.2 Gedanken zum Passwort 343
13.3 Dokumente verschlüsselt speicher 346
13.4 Quick and Dirty mit GnuPG 347
13.4.1 GnuPG für WINDOWS 348
13.5 dm-crypt für Linux 349
13.5.1 Bis zu 8 Passwörter mit LUKS 350
13.5.2 Verschlüsselten Container erstellen 350
13.5.3 Passwörter verwalten 351
13.5.4 Verschlüsselten Container öffnen/schließen 352
13.5.5 Debian GNU/Linux komplett verschlüsseln 355
13.5.6 Ubuntu komplett verschlüsseln 355

13.5.7 HOME-Verzeichnis verschlüsseln 355
13.5.8 SWAP und /tmp verschlüsseln 356
13.6 Backups verschlüsseln 358
13.6.1 Schnell mal auf den USB-Stick 358
13.6.2 Online Backups 361

14 Daten löschen **365**
14.1 Dateien in den Papierkorb werfen 365
14.2 Dateien sicher löschen (Festplatten) 365
14.3 Dateireste nachträglich beseitigen 366
14.4 Dateien sicher löschen (SSDs) 367
14.5 Gesamten Datenträger säubern (Festplatten) 368
14.6 Gesamten Datenträger säubern (SSDs) 369

15 Daten anonymisieren **370**
15.1 Fotos und Bilddateien anonymisieren 371
15.2 PDF-Dokumente säubern 371
15.3 Metadata Anonymisation Toolkit (MAT) für Linux 372

16 Daten verstecken **374**
16.1 Allgemeine Hinweise 375
16.2 steghide 376
16.3 stegdetect 377

17 Betriebssysteme **378**
17.1 Risiko USB, Firewire und Thunderbolt 386
17.2 Linux Firewall konfigurieren 389
17.3 WLAN Privacy Leaks 392
17.3.1 MAC-Adresse faken für Linux 393
17.3.2 MAC-Adresse faken für Windows 10 394
17.3.3 Hostname und DNS-Domain konfigurieren 395

18 Live-DVDs **397**
18.1 USB-Sticks als Bootmedium vorbereiten 397
18.2 BIOS-Einstellungen für Win8+ Rechner 399

19 Smartphones **400**
19.1 Kommerzielle Datensammlungen 401
19.2 Überwachung 403
19.3 Stille SMS ind IMSI-Catcher erkennen 405
19.4 WLAN ausschalten, wenn nicht genutzt 406
19.5 WhatsApp Alternativen 409
19.6 Crypto-Apps 413
19.7 Das Hidden OS im Smartphone 416
19.8 Blackphone 416

Kapitel 1

Scroogled

Greg landete abends um acht auf dem internationalen Flughafen von San Francisco, doch bis er in der Schlange am Zoll ganz vorn ankam, war es nach Mitternacht. Er war der ersten Klasse nussbraun, unrasiert und drahtig entstiegen, nachdem er einen Monat am Strand von Cabo verbracht hatte, um drei Tage pro Woche zu tauchen und sich in der übrigen Zeit mit der Verführung französischer Studentinnen zu beschäftigen. Vor vier Wochen hatte er die Stadt als hängeschultriges, kullerbäuchiges Wrack verlassen. Nun war er ein bronzener Gott, der bewundernde Blicke der Stewardessen vorn in der Kabine auf sich zog.

Vier Stunden später war in der Schlange am Zoll aus dem Gott wieder ein Mensch geworden. Sein Elan war ermattet, Schweiß rann ihm bis hinunter zum Po, und Schultern und Nacken waren so verspannt, dass sein Rücken sich anfühlte wie ein Tennisschläger. Sein iPod-Akku hatte schon längst den Geist aufgegeben, sodass ihm keine andere Ablenkung blieb, als dem Gespräch des Pärchens mittleren Alters vor ihm zu lauschen.

"Die Wunder moderner Technik", sagte die Frau mit Blick auf ein Schild in seiner Nähe: Einwanderung - mit Unterstützung von Google.

"Ich dachte, das sollte erst nächsten Monat losgehen?" Der Mann setzte seinen Riesen-Sombrero immer wieder auf und ab.

Googeln an der Grenze - Allmächtiger. Greg hatte sich vor sechs Monaten von Google verabschiedet, nachdem er seine Aktienoptionen zu Barem gemacht hatte, um sich eine Auszeit zu gönnen, die dann allerdings nicht so befriedigend wurde wie erhofft. Denn während der ersten fünf Monate hatte er kaum etwas anderes getan, als die Rechner seiner Freunde zu reparieren, tagsüber vorm Fernseher zu sitzen und zehn Pfund zuzunehmen - was wohl darauf zurückzuführen war, dass er nun daheim herumsaß statt im Googleplex mit seinem gut ausgestatteten 24-Stunden-Fitnessclub.

Klar, er hätte es kommen sehen müssen. Die US-Regierung hatte 15 Milliarden Dollar daran verschwendet, Besucher an der Grenze zu fotografieren und ihre Fingerabdrücke zu nehmen - und man hatte nicht einen einzigen

Terroristen geschnappt. Augenscheinlich war die öffentliche Hand nicht in der Lage, richtig zu suchen.

Der DHS-Beamte hatte tiefe Ringe unter den Augen und blinzelte auf seinen Monitor, während er die Tastatur mit seinen Wurstfingern traktierte. Kein Wunder, dass es vier Stunden dauerte, aus dem verdammten Flughafen rauszukommen.

"n Abend", sagte Greg und reichte dem Mann seinen schwitzigen Pass. Der Mann grunzte etwas und wischte ihn ab, dann starrte er auf den Bildschirm und tippte. Eine Menge. Ein kleiner Rest getrockneten Essens klebte ihm im Mundwinkel, und er bearbeitete ihn mit seiner Zunge.

"Möchten Sie mir was über Juni 1998 erzählen?"

Greg blickte vom Abflugplan hoch. "Pardon?"

"Sie haben am 17. Juni 1998 eine Nachricht auf alt.burningman über Ihre Absicht geschrieben, ein Festival zu besuchen. Und da fragten Sie: Sind Psychopilze wirklich so eine schlechte Idee?"

Der Interviewer im zweiten Befragungsraum war ein älterer Mann, nur Haut und Knochen, als sei er aus Holz geschnitzt. Seine Fragen gingen sehr viel tiefer als Psychopilze.

"Berichten Sie von Ihren Hobbys. Befassen Sie sich mit Raketenmodellen?"

"Womit?"

"Mit Raketenmodellen."

"Nein", sagte Greg, "überhaupt nicht". Er ahnte, worauf das hinauslief.

Der Mann machte eine Notiz und klickte ein paarmal. "Ich frage nur, weil bei Ihren Suchanfragen und Ihrer Google-Mail ne Menge Werbung für Raketenzubehör auftaucht."

Greg schluckte. "Sie blättern durch meine Suchanfragen und Mails?" Er hatte nun seit einem Monat keine Tastatur angefasst, aber er wusste: Was er in die Suchleiste eintippte, war wahrscheinlich aussagekräftiger als alles, was er seinem Psychiater erzählte.

"Sir, bleiben Sie bitte ruhig. Nein, ich schaue Ihre Suchanfragen nicht an.", sagte der Mann mit einem gespielten Seufzer. "Das wäre verfassungswidrig. Wir sehen nur, welche Anzeigen erscheinen, wenn Sie Ihre Mails lesen oder etwas suchen. Ich habe eine Broschüre, die das erklärt. Sie bekommen sie, sobald wir hier durch sind."

"Aber die Anzeigen bedeuten nichts", platzte Greg heraus. "Ich bekomme Anzeigen für Ann-Coulter-Klingeltöne, sooft ich eine Mail von meinem

Freund in Coulter, Iowa, erhalte!"

Der Mann nickte. "Ich verstehe, Sir. Und genau deshalb spreche ich jetzt hier mit Ihnen. Können Sie sich erklären, weshalb bei Ihnen so häufig Modellraketen-Werbung erscheint?"

Greg grübelte. "Okay, probieren wir es mal. Suchen Sie nach coffee fanatics." Er war in der Gruppe mal ziemlich aktiv gewesen und hatte beim Aufbau der Website ihres Kaffee-des-Monats-Abodienstes geholfen. Die Bohnenmischung zum Start des Angebots hieß "Turbinen-Treibstoff". Das plus "Start", und schon würde Google ein paar Modellraketen-Anzeigen einblenden.

Die Sache schien gerade ausgestanden zu sein, als der geschnitzte Mann die Halloween-Fotos entdeckte - tief vergraben auf der dritten Seite der Suchergebnisse für Greg Lupinski.

"Es war eine Golfkriegs-Themenparty im Castro", sagte er.

"Und Sie sind verkleidet als . . . ?"

"Selbstmordattentäter", erwiderte er kläglich. Das Wort nur auszusprechen verursachte ihm Übelkeit.

"Kommen Sie mit, Mr. Lupinski", sagte der Mann.

Als er endlich gehen durfte, war es nach drei Uhr. Seine Koffer standen verloren am Gepäckkarussell. Er nahm sie und sah, dass sie geöffnet und nachlässig wieder geschlossen worden waren; hier und da lugten Kleidungsstücke heraus.

Daheim stellte er fest, dass all seine pseudopräkolumbianischen Statuen zerbrochen worden waren und dass mitten auf seinem brandneuen weißen mexikanischen Baumwollhemd ein ominöser Stiefelabdruck prangte. Seine Kleidung roch nun nicht mehr nach Mexiko - sie roch nach Flughafen.

An Schlaf war jetzt nicht mehr zu denken, er musste über die Sache reden. Es gab nur eine einzige Person, die all das begreifen würde. Zum Glück war sie normalerweise um diese Zeit noch wach.

Maya war zwei Jahre nach Greg zu Google gekommen. Sie war es, die ihn überzeugt hatte, nach dem Einlösen der Optionen nach Mexiko zu gehen: Wohin auch immer, hatte sie gesagt, solange er nur seinem Dasein einen Neustart verpasste.

Maya hatte zwei riesige schokobraune Labradors und eine überaus geduldige Freundin, Laurie, die mit allem einverstanden war, solange es nicht bedeutete, dass sie selbst morgens um sechs von 350 Pfund sabbernder Caniden durch Dolores Park geschleift wurde.

Maya griff nach ihrem Tränengas, als Greg auf sie zugelaufen kam; dann blickte sie ihn erstaunt an und breitete ihre Arme aus, während sie die Leinen fallen ließ und mit dem Schuh festhielt. “Wo ist der Rest von dir? Mann, siehst du heiß aus!”

Er erwiderte die Umarmung, plötzlich seines Aromas nach einer Nacht invasiven Googelns bewusst. “Maya”, sagte er, “was weißt du über Google und das DHS?”

Seine Frage ließ sie erstarren. Einer der Hunde begann zu jaulen. Sie blickte sich um, nickte dann hoch in Richtung der Tennisplätze. “Auf dem Laternenmast - nicht hinschauen”, sagte sie. “Da ist einer unserer lokalen Funknetz-Hotspots. Weitwinkel-Webcam. Guck in die andere Richtung, während du sprichst.”

Letztlich war es für Google gar nicht teuer gewesen, die Stadt mit Webcams zu überziehen - vor allem, wenn man bedachte, welche Möglichkeiten es bot, Menschen die passende Werbung zu ihrem jeweiligen Aufenthaltsort liefern zu können. Greg hatte seinerzeit kaum Notiz davon genommen, als die Kameras auf all den Hotspots ihren öffentlichen Betrieb aufnahmen; es hatte einen Tag lang Aufruhr in der Blogosphäre gegeben, während die Leute mit dem neuen Allesseher zu spielen begannen und an diverse Rotlichtviertel heranzoomten, doch nach einer Weile war die Aufregung abgeebbt.

Greg kam sich albern vor, er murmelte: “Du machst Witze.”

“Komm mit”, erwiderte sie, nicht ohne sich dabei vom Laternenpfahl abzuwenden.

Die Hunde waren nicht einverstanden damit, den Spaziergang abzukürzen, und taten ihren Unmut in der Küche kund, wo Maya Kaffee zubereitete.

“Wir haben einen Kompromiss mit dem DHS ausgehandelt”, sagte sie und griff nach der Milch. “Sie haben sich damit einverstanden erklärt, nicht mehr unsere Suchprotokolle zu durchwühlen, und wir lassen sie im Gegenzug sehen, welcher Nutzer welche Anzeigen zu sehen bekommt.”

Greg fühlte sich elend. “Warum? Sag nicht, dass Yahoo es schon vorher gemacht hat . . . ”

“N-nein. Doch, ja sicher, Yahoo war schon dabei. Aber das war nicht der Grund für Google mitzumachen. Du weißt doch, die Republikaner hassen Google. Wir sind größtenteils als Demokraten registriert, also tun wir unser Bestes, mit ihnen Frieden zu schließen, bevor sie anfangen, sich auf uns einzuschießen. Es geht ja auch nicht um P.I.I.” - persönlich identifizierende Information, der toxische Smog der Informationsära - “sondern bloß um Metadaten. Also ist es bloß ein bisschen böse.”

“Warum dann all die Heimlichtuerei?”

Maya seufzte und umarmte den Labrador, dessen gewaltiger Kopf auf ihrem Knie ruhte. "Die Schlapphüte sind wie Läuse - die sind überall. Tauchen sogar in unseren Konferenzen auf, als wären wir in irgendeinem Sowjet-Ministerium. Und dann die Sicherheitseinstufungen - das spaltet uns in zwei Lager: solche mit Bescheinigung und solche ohne. Jeder von uns weiß, wer keine Freigabe hat, aber niemand weiß, warum. Ich bin als sicher eingestuft - zum Glück fällt man als Lesbe nicht mehr gleich automatisch durch. Keine sichere Person würde sich herablassen, mit jemandem essen zu gehen, der keine Freigabe hat."

Greg fühlte sich sehr müde. "Na, da kann ich von Glück reden, dass ich lebend aus dem Flughafen herausgekommen bin. Mit Pech wäre ich jetzt eine Vermisstenmeldung, was?"

Maya blickte ihn nachdenklich an. Er wartete auf eine Antwort.

"Was ist denn?"

"Ich werde dir jetzt was erzählen, aber du darfst es niemals weitergeben, o.k.?"

"Ähm, du bist nicht zufällig in einer terroristischen Vereinigung?"

"Wenn es so einfach wäre ... Die Sache ist die: Was das DHS am Flughafen treibt, ist eine Art Vorsortierung, die es den Schlapphüten erlaubt, ihre Suchkriterien enger zu fassen. Sobald du an der Grenze ins zweite Zimmerchen gebeten wirst, bist du *eine Person von Interesse* - und dann haben sie dich im Griff. Sie suchen über Webcams nach deinem Gesicht und Gang, lesen deine Mail, überwachen deine Suchanfragen."

"Sagtest du nicht, die Gerichte würden das nicht erlauben?"

"Sie erlauben es nicht, jedermann undifferenziert auf blauen Dunst zu googeln. Aber sobald du im System bist, wird das eine selektive Suche. Alles legal. Und wenn sie dich erst mal googeln, finden sie garantiert irgendwas. Deine gesamten Daten werden auf *verdächtige Muster* abgegrast, und aus jeder Abweichung von der statistischen Norm drehen sie dir einen Strick."

Greg fühlte Übelkeit in sich aufsteigen. "Wie zum Teufel konnte das passieren? Google war ein guter Ort. *Tu nichts Böses*, war da nicht was?" Das war das Firmenmotto, und für Greg war es ein Hauptgrund dafür gewesen, seinen Stanford-Abschluss in Computerwissenschaften direkten Wegs nach Mountain View zu tragen.

Mayas Erwiderung war ein raues Lachen. "Tu nichts Böses? Ach komm, Greg. Unsere Lobbyistengruppe ist dieselbe Horde von Kryptofaschisten, die Kerry die Swift-Boat-Nummer anhängen wollte. Wir haben schon längst angefangen, vom Bösen zu naschen."

Sie schwiegen eine Minute lang.

“Es ging in China los”, sagte sie schließlich. “Als wir unsere Server aufs Festland brachten, unterstellten wir sie damit chinesischem Recht.”

Greg seufzte. Er wusste nur zu gut um Googles Einfluss: Sooft man eine Webseite mit Google Ads besuchte, Google Maps oder Google Mail benutzte - ja sogar, wenn man nur Mail an einen Gmail-Nutzer sendete -, wurden diese Daten von der Firma penibel gesammelt. Neuerdings hatte Google sogar begonnen, die Suchseite auf Basis solcher Daten für die einzelnen Nutzer zu personalisieren. Dies hatte sich als revolutionäres Marketingwerkzeug erwiesen. Eine autoritäre Regierung würde damit andere Dinge anfangen wollen.

“Sie benutzten uns dazu, Profile von Menschen anzulegen”, fuhr sie fort. “Wenn sie jemanden einbuchten wollten, kamen sie zu uns und fanden einen Vorwand dafür. Schließlich gibt es kaum eine Aktivität im Internet, die in China nicht illegal ist.”

Greg schüttelte den Kopf. “Und warum mussten die Server in China stehen?”

“Die Regierung sagte, sie würde uns sonst blocken. Und Yahoo war schon da.” Sie schnitten beide Grimassen. Irgendwann hatten die Google-Mitarbeiter eine Obsession für Yahoo entwickelt und sich mehr darum gekümmert, was die Konkurrenz trieb, als darum, wie es um das eigene Unternehmen stand. “Also taten wir es - obwohl viele von uns es nicht für eine gute Idee hielten.”

Maya schlürfte ihren Kaffee und senkte die Stimme. Einer ihrer Hunde schnupperte unablässig unter Gregs Stuhl.

“Die Chinesen forderten uns praktisch sofort auf, unsere Suchergebnisse zu zensieren”, sagte Maya. “Google kooperierte. Mit einer ziemlich bizarren Begründung: *Wir tun nichts Böses, sondern wir geben den Kunden Zugriff auf eine bessere Suchmaschine! Denn wenn wir ihnen Suchergebnisse präsentierten, die sie nicht aufrufen können, würde sie das doch nur frustrieren - das wäre ein mieses Nutzererlebnis.*”

“Und jetzt?” Greg schubste einen Hund beiseite. Maya wirkte gekränkt.

“Jetzt bist du eine Person von Interesse, Greg. Du wirst googlebelauert. Du lebst jetzt ein Leben, in dem dir permanent jemand über die Schulter blickt. Denk an die Firmen-Mission: *Die Information der Welt organisieren*. Alles. Lass fünf Jahre ins Land gehen, und wir wissen, wie viele Haufen in der Schüssel waren, bevor du sie gespült hast. Nimm dazu die automatisierte Verdächtigung von jedem, der Übereinstimmungen mit dem statistischen Bild eines Schurken aufweist, und du bist . . . ”

“. . . verraten und vergoogelt.”

"Voll und ganz", nickte sie.

Maya brachte beide Labradors zum Schlafzimmer. Eine gedämpfte Diskussion mit ihrer Freundin war zu hören, dann kam sie allein zurück.

"Ich kann die Sache in Ordnung bringen", presste sie flüsternd hervor. "Als die Chinesen mit den Verhaftungen anfingen, machten ein paar Kollegen und ich es zu unserem 20-Prozent-Projekt, ihnen in die Suppe zu spucken." (Eine von Googles unternehmerischen Innovationen war die Regel, dass alle Angestellten 20 Prozent ihrer Arbeitszeit in anspruchsvolle Projekte nach eigenem Gusto zu investieren hatten.) "Wir nennen es den Googleputzer. Er greift tief in die Datenbanken ein und normalisiert dich statistisch. Deine Suchanfragen, Gmail-Histogramme, Surfmuster. Alles. Greg, ich kann dich googleputzen. Eine andere Möglichkeit hast du nicht."

"Ich will nicht, dass du meinetwegen Ärger bekommst."

Sie schüttelte den Kopf. "Ich bin ohnehin schon geliefert. Jeder Tag, seit ich das verdammte Ding programmiert habe, ist geschenkte Zeit. Ich warte bloß noch drauf, dass jemand dem DHS meinen Background steckt, und dann ... tja, ich weiß auch nicht. Was auch immer sie mit Menschen wie mir machen in ihrem Krieg gegen abstrakte Begriffe."

Greg dachte an den Flughafen, an die Durchsuchung, an sein Hemd mit dem Stiefelabdruck.

"Tu es", sagte er.

Der Googleputzer wirkte Wunder. Greg erkannte es daran, welche Anzeigen am Rand seiner Suchseiten erschienen, Anzeigen, die offensichtlich für jemand anderen gedacht waren. Fakten zum Intelligent Design, Abschluss im Online-Seminar, ein terrorfreies Morgen, Pornografieblocker, die homosexuelle Agenda, billige Toby-Keith-Tickets. Es war offensichtlich, dass Googles neue personalisierte Suche ihn für einen völlig anderen hielt: einen gottesfürchtigen Rechten mit einer Schwäche für Cowboy-Musik.

Nun gut, das sollte ihm recht sein.

Dann klickte er sein Adressbuch an und stellte fest, dass die Hälfte seiner Kontakte fehlte. Sein Gmail-Posteingang war wie von Termiten ausgehöhlt, sein Orkut-Profil normalisiert. Sein Kalender, Familienfotos, Lesezeichen: alles leer. Bis zu diesem Moment war ihm nicht klar gewesen, wie viel seiner selbst ins Web migriert war und seinen Platz in Googles Serverfarmen gefunden hatte - seine gesamte Online-Identität. Maya hatte ihn auf Hochglanz poliert; er war jetzt Der Unsichtbare.

Greg tippte schläfrig auf die Tastatur seines Laptops neben dem Bett und erweckte den Monitor zum Leben. Er blinzelte die Uhr in der Toolbar an. 4:13 Uhr morgens! Allmächtiger, wer hämmerte denn um diese Zeit gegen seine Tür?

Er rief mit nuscheliger Stimme "Komm ja schon" und schlüpfte in Morgenmantel und Pantoffeln. Dann schlurfte er den Flur entlang und knipste unterwegs die Lichter an. Durch den Türspion blickte ihm düster Maya entgegen.

Er entfernte Kette und Riegel und öffnete die Tür. Maya huschte an ihm vorbei, gefolgt von den Hunden und ihrer Freundin. Sie war schweißüberströmt, ihr normalerweise gekämmtes Haar hing strähnig in die Stirn. Sie rieb sich die roten, geränderten Augen.

"Pack deine Sachen", stieß sie heiser hervor.

"Was?"

Sie packte ihn bei den Schultern. "Mach schon", sagte sie.

"Wohin willst . . . "

"Mexiko wahrscheinlich. Weiß noch nicht. Nun pack schon, verdammt." Sie drängte sich an ihm vorbei ins Schlafzimmer und begann, Schubladen zu öffnen.

"Maya", sagte er scharf, "ich gehe nirgendwohin, solange du mir nicht sagst, was los ist."

Sie starrte ihn an und wischte ihre Haare aus dem Gesicht. "Der Googleputzer lebt. Als ich dich gesäubert hatte, habe ich ihn runtergefahren und bin verschwunden. Zu riskant, ihn noch weiter zu benutzen. Aber er schickt mir Mailprotokolle, sooft er läuft. Und jemand hat ihn sechs Mal verwendet, um drei verschiedene Benutzerkonten zu schrubben - und die gehören zufällig alle Mitgliedern des Senats-Wirtschaftskomitees, die vor Neuwahlen stehen."

"Googler frisieren die Profile von Senatoren?"

"Keine Google-Leute. Das kommt von außerhalb; die IP-Blöcke sind in D.C. registriert. Und alle IPs werden von Gmail-Nutzern verwendet. Rate mal, wem diese Konten gehören."

"Du schnüffelst in Gmail-Konten?"

"Hm, ja. Ich habe durch ihre E-Mails geschaut. Jeder macht das mal, und mit weitaus übleren Motiven als ich. Aber stell dir vor, all diese Aktivität geht von unserer Lobbyistenfirma aus. Machen nur ihren Job, dienen den Interessen des Unternehmens."

Greg fühlte das Blut in seinen Schläfen pulsieren. "Wir sollten es jemandem erzählen."

"Das bringt nichts. Die wissen alles über uns. Sehen jede Suchanfrage, jede Mail, jedes Mal, wenn uns die Webcams erfassen. Wer zu unserem sozialen Netzwerk gehört ... Wusstest du das? Wenn du 15 Orkut-Freunde hast, ist es statistisch gesehen sicher, dass du höchstens drei Schritte entfernt bist von jemandem, der schon mal Geld für *terroristische Zwecke* gespendet hat. Denk an den Flughafen - das war erst der Anfang für dich."

"Maya", sagte Greg, der nun seine Fassung wiedergewann, "übertreibst du es nicht mit Mexiko? Du könntest doch kündigen, und wir ziehen ein Start-up auf. Aber das ist doch bescheuert."

"Sie kamen heute zu Besuch", entgegnete sie. "Zwei politische Beamte vom DHS. Blieben stundenlang und stellten eine Menge verdammt harter Fragen."

"Über den Googleputzer?"

"Über meine Freunde und Familie. Meine Such-Geschichte. Meine persönliche Geschichte."

"Jesus."

"Das war eine Botschaft für mich. Die beobachten mich - jeden Klick, jede Suche. Zeit zu verschwinden, jedenfalls aus ihrer Reichweite."

"In Mexiko gibt es auch eine Google-Niederlassung."

"Wir müssen jetzt los", beharrte sie.

"Laurie, was hältst du davon?", fragte Greg.

Laurie stupste die Hunde zwischen die Schultern. "Meine Eltern sind 65 aus Ostdeutschland weggegangen. Sie haben mir immer von der Stasi erzählt. Die Geheimpolizei hat alles über dich in deiner Akte gesammelt: ob du vaterlandsfeindliche Witze erzählst, all son Zeug. Ob sie es nun wollten oder nicht, Google hat inzwischen das Gleiche aufgezogen."

"Greg, kommst du nun?"

Er blickte die Hunde an und schüttelte den Kopf. "Ich habe ein paar Pesos übrig", sagte er. "Nehmt sie mit. Und passt auf euch auf, ja?"

Maya zog ein Gesicht, als wolle sie ihm eine runterhauen. Dann entspannte sie sich und umarmte ihn heftig.

"Pass du auf dich auf", flüsterte sie ihm ins Ohr.

Eine Woche später kamen sie zu ihm. Nach Hause, mitten in der Nacht, genau wie er es sich vorgestellt hatte. Es war kurz nach zwei Uhr morgens, als

zwei Männer vor seiner Tür standen.

Einer blieb schweigend dort stehen. Der andere war ein Lächler, klein und faltig, mit einem Fleck auf dem einen Mantelrevers und einer amerikanischen Flagge auf dem anderen. “Greg Lupinski, es besteht der begründete Verdacht, dass Sie gegen das Gesetz über Computerbetrug und -missbrauch verstoßen haben”, sagte er, ohne sich vorzustellen. “Insbesondere, dass Sie Bereiche autorisierten Zugangs überschritten und sich dadurch Informationen verschafft haben. Zehn Jahre für Ersttäter. Außerdem gilt das, was Sie und Ihre Freundin mit Ihren Google-Daten gemacht haben, als schweres Verbrechen. Und was dann noch in der Verhandlung zutage kommen wird ... angefangen mit all den Dingen, um die Sie Ihr Profil bereinigt haben.”

Greg hatte diese Szene eine Woche lang im Geist durchgespielt, und er hatte sich allerlei mutige Dinge zurechtgelegt, die er hatte sagen wollen. Es war eine willkommene Beschäftigung gewesen, während er auf Mayas Anruf wartete. Der Anruf war nie gekommen.

“Ich möchte einen Anwalt sprechen”, war alles, was er herausbrachte.

“Das können Sie tun”, sagte der kleine Mann. “Aber vielleicht können wir zu einer besseren Einigung kommen.”

Greg fand seine Stimme wieder. “Darf ich mal Ihre Marke sehen?”

Das Basset-Gesicht des Mannes hellte sich kurz auf, als er ein amüsiertes Glucksen unterdrückte. “Kumpel, ich bin kein Bulle”, entgegnete er. “Ich bin Berater. Google beschäftigt mich - meine Firma vertritt ihre Interessen in Washington -, um Beziehungen aufzubauen. Selbstverständlich würden wir niemals die Polizei hinzuziehen, ohne zuerst mit Ihnen zu sprechen. Genau genommen möchte ich Ihnen ein Angebot unterbreiten.”

Greg wandte sich der Kaffeemaschine zu und entsorgte den alten Filter.

“Ich gehe zur Presse”, sagte er.

Der Mann nickte, als ob er darüber nachdenken müsse. “Na klar. Sie gehen eines Morgens zum Chronicle und breiten alles aus. Dort sucht man nach einer Quelle, die Ihre Story stützt; man wird aber keine finden. Und wenn sie danach suchen, werden wir sie finden. Also lassen Sie mich doch erst mal ausreden, Kumpel. Ich bin im Win-Win-Geschäft, und ich bin sehr gut darin.”

Er pausierte. “Sie haben da übrigens hervorragende Bohnen, aber wollen Sie sie nicht erst eine Weile wässern? Dann sind sie nicht mehr so bitter, und die Öle kommen besser zur Geltung. Reichen Sie mir mal ein Sieb?”

Greg beobachtete den Mann dabei, wie er schweigend seinen Mantel auszog und über den Küchenstuhl hängte, die Manschetten öffnete, die Ärmel sorgfältig hochrollte und eine billige Digitaluhr in die Tasche steckte. Er kippte

die Bohnen aus der Mühle in Gregs Sieb und wässerte sie in der Spüle.

Er war ein wenig untersetzt und sehr bleich, mit all der sozialen Anmut eines Elektroingenieurs. Wie ein echter Googler auf seine Art, besessen von Kleinigkeiten. Mit Kaffeemühlen kannte er sich also auch aus.

"Wir stellen ein Team für Haus 49 zusammen . . . "

"Es gibt kein Haus 49", sagte Greg automatisch.

"Schon klar", entgegnete der andere mit verkniffenem Lächeln. "Es gibt kein Haus 49. Aber wir bauen ein Team auf, das den Googleputzer überarbeiten soll. Mayas Code war nicht sonderlich schlank und steckt voller Fehler. Wir brauchen ein Upgrade. Sie wären der Richtige; und was Sie wissen, würde keine Rolle spielen, wenn Sie wieder an Bord sind."

"Unglaublich", sagte Greg spöttisch. "Wenn Sie denken, dass ich Ihnen helfe, im Austausch für Gefälligkeiten politische Kandidaten anzuschwärzen, sind Sie noch wahnsinniger, als ich dachte."

"Greg", sagte der Mann, "niemand wird angeschwärzt. Wir machen nur ein paar Dinge sauber. Für ausgewählte Leute. Sie verstehen mich doch? Genauer betrachtet gibt jedes Google-Profil Anlass zur Sorge. Und genaue Betrachtung ist der Tagesbefehl in der Politik. Eine Bewerbung um ein Amt ist wie eine öffentliche Darmspiegelung." Er befüllte die Kaffeemaschine und drückte mit vor Konzentration verzerrtem Gesicht den Kolben nieder. Greg holte zwei Kaffeetassen (Google-Becher natürlich) und reichte sie weiter.

"Wir tun für unsere Freunde das Gleiche, was Maya für Sie getan hat. Nur ein wenig aufräumen. Nur ihre Privatsphäre schützen - mehr nicht."

Greg nippte am Kaffee. "Was geschieht mit den Kandidaten, die Sie nicht putzen?"

"Na ja", sagte Gregs Gegenüber mit dünnem Grinsen, "tja, Sie haben Recht, für die wird es ein bisschen schwierig." Er kramte in der Innentasche seines Mantels und zog einige gefaltete Blätter Papier hervor, strich sie glatt und legte sie auf den Tisch. "Hier ist einer der Guten, der unsere Hilfe braucht." Es war das ausgedruckte Suchprotokoll eines Kandidaten, dessen Kampagne Greg während der letzten drei Wahlen unterstützt hatte.

"Der Typ kommt also nach einem brutalen Wahlkampf-Tag voller Klinkenputzen ins Hotel, fährt den Laptop hoch und tippt *knackige Ärsche* in die Suchleiste. Ist doch kein Drama, oder? Wir sehen es so: Wenn man wegen so was einen guten Mann daran hindert, weiterhin seinem Land zu dienen, wäre das schlichtweg unamerikanisch."

Greg nickte langsam.

“Sie werden ihm also helfen?”, fragte der Mann.

“Ja.”

“Gut. Da wäre dann noch was: Sie müssen uns helfen, Maya zu finden. Sie hat überhaupt nicht verstanden, worum es uns geht, und jetzt scheint sie sich verdrückt zu haben. Wenn sie uns bloß mal zuhört, kommt sie bestimmt wieder rum.”

Er betrachtete das Suchprofil des Kandidaten.

“Denke ich auch”, erwiderte Greg.

Der neue Kongress benötigte elf Tage, um das Gesetz zur Sicherung und Erfassung von Amerikas Kommunikation und Hypertext zu verabschieden. Es erlaubte dem DHS und der NSA, bis zu 80 Prozent der Aufklärungs- und Analysearbeit an Fremdfirmen auszulagern. Theoretisch wurden die Aufträge über offene Bietverfahren vergeben, aber in den sicheren Mauern von Googles Haus 49 zweifelte niemand daran, wer den Zuschlag erhalten würde. Wenn Google 15 Milliarden Dollar für ein Programm ausgegeben hätte, Übeltäter an den Grenzen abzufangen, dann hätte es sie garantiert erwischt - Regierungen sind einfach nicht in der Lage, richtig zu suchen.

Am Morgen darauf betrachtete Greg sich prüfend im Rasierspiegel (das Wachpersonal mochte keine Hacker-Stoppelbärte und hatte auch keine Hemmungen, das deutlich zu sagen), als ihm klar wurde, dass heute sein erster Arbeitstag als De-facto-Agent der US-Regierung begann. Wie schlimm mochte es werden? Und war es nicht besser, dass Google die Sache machte, als irgendein ungeschickter DHS-Schreibtischtäter?

Als er am Googleplex zwischen all den Hybridautos und überquellenden Fahrradständern parkte, hatte er sich selbst überzeugt. Während er sich noch fragte, welche Sorte Bio-Fruchtshake er heute in der Kantine bestellen würde, verweigerte seine Codekarte den Zugang zu Haus 49. Die rote LED blinkte immer nur blöde vor sich hin, wenn er seine Karte durchzog. In jedem anderen Gebäude würde immer mal jemand raus- und wieder reinkommen, dem man sich anschließen könnte. Aber die Googler in 49 kamen höchstens zum Essen raus, und manchmal nicht einmal dann.

Ziehen, ziehen, ziehen. Plötzlich hörte er eine Stimme neben sich.

“Greg, kann ich Sie bitte sprechen?”

Der verschrumpelte Mann legte einen Arm um seine Schulter, und Greg atmete den Duft seines Zitrus-Rasierwassers ein. So hatte sein Tauchlehrer in Baja geduftet, wenn sie abends durch die Kneipen zogen. Greg konnte sich nicht an seinen Namen erinnern: Juan Carlos? Juan Luis?

Der Mann hielt seine Schulter fest im Griff, lotste ihn weg von der Tür, über den tadellos getrimmten Rasen und vorbei am Kräutergarten vor der

Küche. “Wir geben Ihnen ein paar Tage frei”, sagte er.

Greg durchschoss eine Panikattacke. “Warum?” Hatte er irgendetwas falsch gemacht? Würden sie ihn einbuchten?

“Es ist wegen Maya.” Der Mann drehte ihn zu sich und begegnete ihm mit einem Blick endloser Tiefe. “Sie hat sich umgebracht. In Guatemala. Es tut mir Leid, Greg.”

Greg spürte, wie der Boden unter seinen Füßen verschwand und wie er meilenweit emporgezogen wurde. In einer Google-Earth-Ansicht des Googleplex sah er sich und den verschrumpelten Mann als Punktepaar, zwei Pixel, winzig und belanglos. Er wünschte, er könnte sich die Haare ausreißen, auf die Knie fallen und weinen.

Von weit, weit weg hörte er sich sagen: “Ich brauche keine Auszeit. Ich bin okay.”

Von weit, weit weg hörte er den verschrumpelten Mann darauf bestehen.

Die Diskussion dauerte eine ganze Weile, dann gingen die beiden Pixel in Haus 49 hinein, und die Tür schloss sich hinter ihnen.

Ich danke dem Autor Cory Doctorow und dem Übersetzer Christian Wöhrl dafür, dass sie den Text unter einer Creativ Commons Lizenz zur Nutzung durch Dritte bereitstellen.

Kapitel 2

Angriffe auf die Privatsphäre

Im realen Leben ist Anonymität die tagtäglich erlebte Erfahrung. Wir gehen eine Straße enlang, kaufen eine Zeitung, ohne uns ausweisen zu müssen, beim Lesen der Zeitung schaut uns niemand zu. Das Aufgeben von Anonymität (z.B. mit Rabattkarten) ist eine aktive Entscheidung.

Im Internet ist es genau umgekehrt. Von jedem Nutzer werden Profile erstellt. Webseitenbetreiber sammeln Informationen (Surfverhalten, E-Mail-Adressen), um beispielsweise mit dem Verkauf der gesammelten Daten ihr Angebot zu finanzieren. Betreiber von Werbe-Servern nutzen die Möglichkeiten, das Surfverhalten webseitenübergreifend zu erfassen.

Verglichen mit dem Beispiel *Zeitunglesen* läuft es auf dem Datenhighway so, dass uns Zeitungen in großer Zahl kostenlos aufgedrängt werden. Beim Lesen schaut uns ständig jemand über die Schulter, um unser Interessen- und Persönlichkeitsprofil für die Einblendung passender Werbung zu analysieren oder um es zu verkaufen (z.B. an zukünftige Arbeitgeber). Außerdem werden unsere Kontakte zu Freunden ausgewertet, unsere Kommunikation wird gescannt, Geheimdienste sammeln kompromittierendes Material...

Neben den Big Data Firmen werden auch staatliche Maßnahmen zur Überwachung derzeit stark ausgebaut und müssen von Providern unterstützt werden. Nicht immer sind die vorgesehenen Maßnahmen rechtlich unbedenklich.

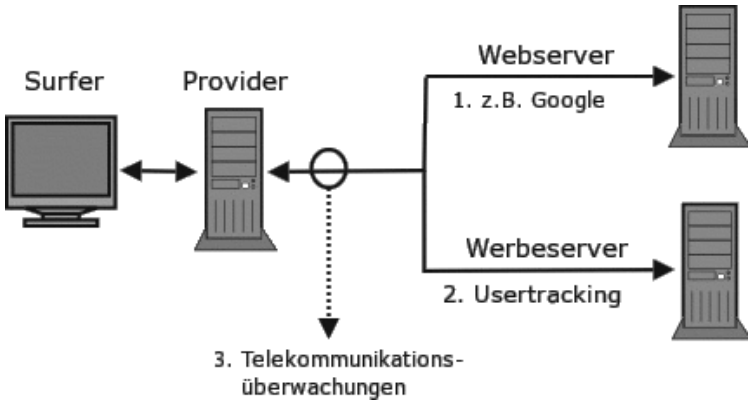


Abbildung 2.1: Möglichkeiten zur Überwachung im WWW

2.1 Big Data - Kunde ist der, der bezahlt

Viele Nutzer dieser Dienste sehen sich in der Rolle von *Kunden*. Das ist falsch. Kunde ist der, der bezahlt. Kommerzielle Unternehmen (insbesondere börsennotierte Unternehmen) optimieren ihre Webangebote, um den zahlenden Kunden zu gefallen und den Gewinn zu maximieren. Die vielen Freibier-Nutzer sind bestenfalls *glückliche Hamster im Laufrad*, die die verkaufte Ware produzieren.

2.1.1 Google

Das Beispiel Google wurde aufgrund der Bekanntheit gewählt. Auch andere Firmen gehören zu den Big Data Companies und versuchen mit ähnlichen Geschäftsmodellen Gewinne zu erzielen. Im Gegensatz zu Facebook, Twitter... usw. verkauft Google die gesammelten Informationen über Nutzer nicht an Dritte sondern verwendet sie intern für Optimierung der Werbung. Nur an die NSA werden nach Informationen des Whistleblowers W. Binney zukünftig Daten weitergegeben.

Wirtschaftliche Zahlen

Google hat einen jährlichen Umsatz von 37 Milliarden Dollar, der ca. 9,4 Milliarden Dollar Gewinn abwirft. 90% des Umsatzes erzielt Google mit personalisierter Werbung. Die Infrastruktur kostet ca. 2 Millarden Dollar jährlich. (Stand: 2011)

Google Web Search

Googles Websuche ist in Deutschland die Nummer Eins. 89% der Suchanfragen gehen direkt an *google.de*. Mit den Suchdiensten wie Ixquick, Metager2, Web.de... die indirekt Anfragen an Google weiterleiten, beantwortet der Primus ca. 95% der deutschen Suchanfragen. (Stand 2008)

1. Laut Einschätzung der Electronic Frontier Foundation werden alle Suchanfragen protokolliert und die meisten durch Cookies, IP-Adressen und Informationen von Google Accounts einzelnen Nutzern zugeordnet.

   In den Datenschutzbestimmungen von Google kann man nachlesen, dass diese Informationen (in anonymisierter Form) auch an Dritte weitergegeben werden. Eine Einwilligung der Nutzer in die Datenweitergabe liegt nach Ansicht der Verantwortlichen vor, da mit der Nutzung des Dienstes auch die AGBs akzeptiert wurden. Sie sind schließlich auf der Website öffentlich einsehbar.

2. Nicht nur die Daten der Nutzer werden analysiert. Jede Suchanfrage und die Reaktionen auf die angezeigten Ergebnisse werden protokolliert und ausgewertet.

   Google Flu Trends zeigt, wie gut diese Analyse der Suchanfragen bereits arbeitet. Anhand der Such-Protokolle wird eine Ausbreitung der Grippe um 1-2 Wochen schneller erkannt, als es bisher dem U.S. Center for Disease Control and Prevention möglich war.

   Die mathematischen Grundlagen für diese Analysen wurden im Rahmen der Bewertung von Googles 20%-Projekten entwickelt. Bis 2008 konnten Entwickler bei Google 20% ihrer Arbeitszeit für eigene Ideen verwenden. Interessante Ansätze aus diesem Umfeld gingen als Beta-Version online (z.B. Orkut). Die Reaktionen der Surfer auf diese Angebote wurde genau beobachtet. Projekte wurden wieder abgeschaltet, wenn sie die harten Erfolgskriterien nicht erfüllten (z.B. Google Video).

   Inzwischen hat Google die 20%-Klausel abgeschafft. Die Kreativität der eigenen Mitarbeiter ist nicht mehr notwendig und zu teuer. Diese Änderung der Firmenpolitik wird von einer Fluktuation des Personals begleitet. 30% des kreativen Stammpersonals von 2000 haben der Firma inzwischen den Rücken zugekehrt. (Stand 2008)

   Die entwickelten Bewertungsverfahren werden zur Beobachtung der Trends im Web eingesetzt. Der Primus unter den Suchmaschinen ist damit in der Lage, erfolgversprechende Ideen und Angebote schneller als andere Mitbewerber zu erkennen und darauf zu reagieren. Die Ideen werden nicht mehr selbst entwickelt, sondern aufgekauft und in das Imperium integriert. Seit 2004 wurden 60 Firmen übernommen, welche zuvor die Basis für die meisten aktuellen Angebote von Google entwickelt hatten: Youtube, Google Docs, Google Maps, Google Earth, Google Analytics, Picasa, SketchUp, die Blogger-Plattformen...

   Das weitere Wachstum des Imperiums scheint langfristig gesichert.

   Zu spät hat die Konkurrenz erkannt, welches enorme Potential die Auswertung von Suchanfragen darstellt. Mit dem Börsengang 2004 musste

Google seine Geheimniskrämerei etwas lockern und für die Börsenaufsicht Geschäftsdaten veröffentlichen. Microsoft hat daraufhin Milliaden Dollar in *MSN Live Search, Bing* versenkt und Amazon, ein weiterer Global Player im Web, der verniedlichend als Online Buchhändler bezeichnet wird, versuchte mit *A9* ebenfalls eine Suchmaschine zu etablieren.

Adsense, DoubleClick, Analytics & Co.

Werbung ist die Haupteinnahmequelle von Google. Im dritten Quartal 2010 erwirtschaftete Google 7,3 Milliarden Dollar und damit 97% der Einnahmen aus Werbung. Zielgenaue Werbung basierend auf umfassenden Informationen über Surfer bringt wesentlich höhere Einkünfte, als einfache Bannerschaltung. Deshalb sammeln Werbetreibende im Netz umfangreiche Daten über Surfer. Es wird beispielsweise verfolgt, welche Webseiten ein Surfer besucht und daraus ein Interessenprofil abgeleitet. Die Browser werden mit geeigneten Mitteln markiert (Cookies u.ä.), um Nutzer leichter wieder zu erkennen.

Inzwischen lehnen 84% der Internetnutzer dieses Behavioral Tracking ab. Von den Unternehmen im Internet wird es aber stetig ausgebaut. Google ist auf diesem Gebiet führend und wird dabei (unwissentlich?) von vielen Websitebetreibern unterstützt.

97% der TOP100 Websites und ca. 80% der deutschsprachigen Webangebote sind mit verschiedenen Elementen von Google für die Einblendung kontextsensitiver Werbung und Traffic-Analyse infiziert! (Reppesgaard: Das Google Imperium, 2008) Jeder Aufruf einer derart präparierten Website wird bei Google registriert, ausgewertet und einem Surfer zugeordnet. Neben kommerziellen Verkaufs-Websites, Informationsangeboten professioneller Journalisten und Online-Redaktionen gehören die Websites politischer Parteien genauso dazu, wie unabhängige Blogger auf den Plattformen *blogger.com* und *blogspot.com* sowie private Websites, die sich über ein paar Groschen aus dem Adsense-Werbe-Programm freuen.

Untragbar wird diese Datenspionage, wenn politische Parteien wie die CSU ihre Spender überwachen lassen. Die CSU bietet ausschließlich die Möglichkeit, via Paypal zu spenden. Die Daten stehen damit inklusive Wohnanschrift und Kontonummer einem amerikanischen Großunternehmen zur Verfügung. Außerdem lässt die CSU ihre Spender mit Google-Analytics beobachten. Der Datenkrake erhält damit eindeutige Informationen über politische Anschauungen. Diese Details können im Informationskrieg wichtig sein.

Damit kennt das Imperium nicht nur den Inhalt der Websites, die vom Google-Bot für den Index der Suchmaschine abgeklappert wurden. Auch Traffic und Besucher der meisten Websites sind bekannt. Diese Daten werden Werbetreibenden anonymisiert zur Verfügung gestellt.

Die Grafik in Abb. 2.2 zur Besucherstatistik wurde vom Google Ad-Planner für eine (hier nicht genannte) Website erstellt. Man erkennt, dass der überwiegende Anteil der Besucher männlich und zwischen 35-44 Jahre alt ist. Die Informationen zu Bildung und Haushaltseinkommen müssen im Vergleich

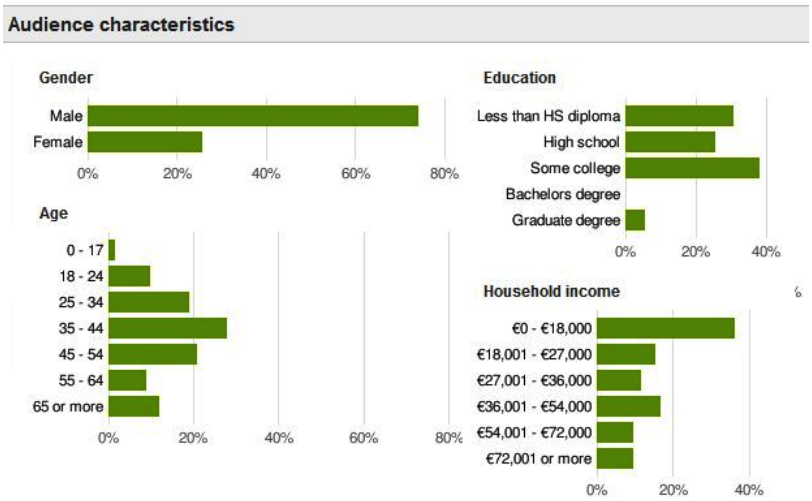


Abbildung 2.2: Ad-Planner Besucherstatistik (Beispiel)

zu allgemeinen Statistiken der Bevölkerung bewertet werden, was hier mal entfällt.

Wie kommt das Imperium zu diesen Daten? Es gibt so gut wie keine Möglickheit, diese Daten irgendwo einzugeben. Google fragt NICHT nach diesen Daten, sie werden aus der Analyse des Surf- und Suchverhaltens gewonnen. Zusätzlich kauft Google bei Marktforschungsunternehmen große Mengen an Informationen, die in die Kalkulation einfließen.

Wenn jemand mit dem iPhone auf der Website von BMW die Preise von Neuwagen studiert, kann Google ihn einer Einkommensgruppe zuordnen. Wird der Surfer später beim Besuch von Spiegel-Online durch Einblendung von Werbung wiedererkannt, kommt ein entsprechender Vermerk in die Datenbank. Außerdem kann die Werbung passend zu seinen Interessen und Finanzen präsentiert werden. Die Realität ist natürlich etwas komplexer.

Mit dem im April 2010 eingeführtem **Retargeting** geht Google noch weiter. Mit Hilfe spezieller Cookies werden detaillierte Informationen über Surfer gesammelt. Die Informationen sollen sehr genau sein, bis hin zu Bekleidungsgrößen, für die man sich in einem Webshop interessiert hat. Die gesammelten Informationen sollen die Basis für punktgenaue Werbung bieten. Beispielsweise soll nach dem Besuch eines Webshops für Bekleidung ohne Kaufabschluss permanent alternative Werbung zu diesem Thema eingeblendet werden.

Google Mail, Talk, News... und Google+ (personalisierte Dienste)

Mit einem einheitlichem Google-Konto können verschiedene personalisierte Angebote genutzt werden. (Google Mail, News, Talk, Calendar, Alert, Orkut, Börsennachrichten..... iGoogle)

Bei der Anmeldung ist das Imperium weniger wissbegierig, als vergleichbare kommerzielle Anbieter. Vor- und Nachname, Login-Name und Passwort reichen aus. Es ist nicht unbedingt nötig, seinen realen Namen anzugeben. Ein Pseudonym wird auch akzeptiert. Die Accounts ermöglichen es, aus dem Surf- und Suchverhalten, den zusammengestellten Nachrichtenquellen, dem Inhalt der E-Mails usw. ein Profil zu erstellen. Die unsichere Zuordnung über Cookies, IP-Adressen und andere Merkmale ist nicht nötig. Außerdem dienen die Dienste als Flächen für personalisierte und gut bezahlte Werbung.

Patente aus dem Umfeld von Google Mail zeigen, dass dabei nicht nur Profile über die Inhaber der Accounts erstellt werden, sondern auch die Kommunikationspartner unter die Lupe genommen werden. Wer an einen Google Mail Account eine E-Mail sendet, landet in der Falle des Datenkraken.

Die Einrichtung eines Google-Accounts ermöglicht es aber auch, gezielt die gesammelten Daten in gewissem Umfang zu beeinflussen. Man kann Einträge aus der Such- und Surf-Historie löschen u.ä. (Besser ist es sicher, die Einträge von vornherein zu vermeiden.)

Smartphones und Android

2005 hat Google die Firma Android Inc. für 50 Mio. Dollar gekauft und sucht mit dem Smartphone Betriebssystem Android auf dem Markt der mobilen Kommunikation ähnliche Erfolge wie im Web.

Bei der Nutzung von Android Smartphones sollen alle E-Mails über Google Mail laufen, Termine mit dem Google Calendar abgeglichen werden, die Kontaktdaten sollen bei Google landen... Die Standortdaten werden ständig an Google übertragen, um sogenannte Mehrwertdienste bereit zu stellen (genau wie das iPhone die Standortdaten an Apple sendet). Smartphones sind als Livestyle-Gadget getarnte Tracking Devices.

> *Wir wissen, wo u bist. Wir wissen, wo du warst. Wir können mehr oder weniger wissen, was du gerade denkst.* (Google-Chef Eric Schmidt, 2010)

Mozilla Firefox

Google ist der Hauptsponsor der Firefox Entwickler. Seit 2012 zahlt Google jährlich 300 Mio. Dollar an die Mozilla Foundation, um die voreingestellte Standardsuchmaschine in diesem Browser zu sein.

Das ist natürlich in erster Linie ein Angriff auf Microsoft. Die Entwickler von Firefox kommen ihrem datensammelnden Hauptsponsor jedoch in vielen Punkten deutlich entgegen:

- Die Default-Startseite ermöglicht es Google, ein langlebiges Cookie im First-Party Context zu setzen und den Browser damit praktisch zu personalisieren. Die standardmäßig aktive Richtline für Cookies ermöglicht

es Google exklusive, auch als Drittseite das Surfverhalten zu verfolgen, da mit dem Start ein Cookie vorhanden ist.

- Sollte die Startseite modifiziert worden sein (z.B. bei der Variante *Iceweasel* von Debian GNU/Linux oder bei Ubuntu), erfolgt die "Personalisierung" des Browsers wenige Minuten später durch Aktualisierung der Phishing-Datenbank.

- Diese "Personalisierung" ermöglicht es Google, den Nutzer auf allen Webseiten zu erkennen, die mit Werbeanzeigen aus dem Imperium oder Google-Analytics verschmutzt sind. Im deutschsprachigen Web hat sich diese Verschmutzung auf 4/5 der relevanten Webseiten ausgebreitet.

(Trotzdem ist Mozilla Firefox ein guter Browser. Mit wenigen Anpassungen und Erweiterungen von unabhängigen Entwicklern kann man ihm die Macken austreiben und spurenarm durchs Web surfen.)

Google DNS

Mit dem DNS-Service versucht Google, die Digital Natives zu erreichen. Der Service spricht Nerds an, die in der Lage sind, Cookies zu blockieren, Werbung auszublenden und die natürlich einen DNS-Server konfigurieren können.

Google verspricht, dass die DNS-Server unter den IP-Adressen 8.8.8.8 und 8.8.4.4 nicht kompromittiert oder zensiert werden und bemüht sich erfolgreich um schnelle DNS-Antworten. Die Google-Server sind etwa 1/10 sec bis 1/100 sec schneller als andere unzensierte DNS-Server.

Natürlich werden alle Anfragen gespeichert und ausgewertet. Ziel ist, die von erfahrenen Nutzern besuchten Websites zu erfassen und in das Monitoring des Web besser einzubeziehen. Positiv an dieser Initiative ist, dass es sich kaum jemand leisten kann, die Wirtschaftsmacht Google zu blockieren. Damit wird auch die Sperrung alternativer DNS-Server, wie es in Deutschland im Rahmen der Einführung der Zensur geplant war, etwas erschwert.

Kooperation mit Geheimdiensten (NSA, CIA)

Es wäre verwunderlich, wenn die gesammelten Datenbestände nicht das Interesse der Geheimdienste wecken würden. Das EPIC bemühte sich jahrlang auf Basis des Freedom of Information Act, Licht in diese Kooperation zu bringen. Die Anfragen wurden nicht beantwortet.[1]

Erst durch die von Snowden/Greenwald veröffentlichten Dokumente wurde mehr bekannt. Google ist seit 2009 einer der ersten PRISM-Partner der NSA. Das bedeutet, dass der US-Geheimdienst vollen Zugriff auf die Daten der Nutzer hat. Von allen auf der Folie genannten PRISM-Firmen wurden über-spezifische Dementis veröffentlicht, dass sie nie von einem Programm mit dem Namen PRISM gehört hätten und demzufolge nicht wissentlich mit der NSA im Rahmen von PRISM kooperieren würden. Rajesh De, Leiter

[1] http://epic.org/2010/09/epic-files-suit-for-documents.html

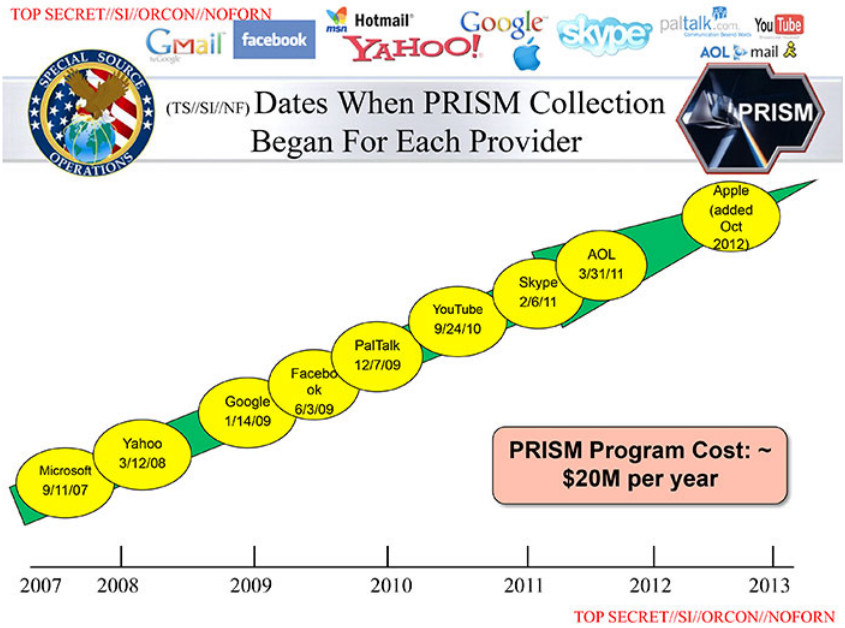


Abbildung 2.3: NSA-Folie zu den PRISM-Partnern

der Rechtsabteilung der NSA, dementierte die Dementis[2] und stellte klar, dass die Internetfirmen zwar den intern verwendetet Namen PRISM nicht kannten, dass die Datensammlung aber mit *voller Kenntnis und Unterstützung* der Unternehmen erfolgte.

Das Dementi von Google ist außerdem aufgrund der Informationen des Whistleblowers W. Binney unglaubwürdig. W. Binney war 30 Jahre in führenden Positionen der NSA tätig und veröffentlichte 2012, dass Google Kopien des gesamten E-Mail Verkehrs von GMail und sämtliche Suchanfragen dem neuen Datacenter der NSA in Bluffdale zur Verfügung stellen wird:

> *It will store all Google search queries, e-mail and fax traffic.*

Wenn Googles Verwaltungsratschef Eric Schmidt auf der SXSW-Konferenz 2014 behauptet, durch Einführung der SSL-Verschlüsselung zwischen Datencentern seien die Daten der Google-Nutzer jetzt vor der NSA sicher[3], dann kann man es als PR-Gag abtun. Google ist aufgrund geltender Gesetze zur Kooperation mit den weitreichenden Späh-Programmen der NSA verpflichtet.

Außerdem kooperiert Google mit der CIA bei der Auswertung der Datenbestände im Rahmen des Projektes Future of Web Monitoring, um Trends zu erkennen und für die Geheimdienste der USA zu erschließen.

[2] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google-yahoo-co-nsa-anwalt-internetfirmen-wussten-von-ausspaehaktionen-12855553.html

[3] https://heise.de/-2138499

Kooperation mit Behörden

Auf Anfrage stellt Google den Behörden der Länder die angeforderten Daten zur Verfügung. Dabei agiert Google auf Grundlage der nationalen Gesetze. Bei daten-speicherung.de findet man Zahlen zur Kooperationswilligkeit des Imperiums. Durchschnittlich beantwortet Google Anfragen mit folgender Häufigkeit:

- 3mal täglich von deutschen Stellen
- 20mal täglich von US-amerikanischen Stellen
- 6mal täglich von britischen Stellen

In den drei Jahren von 2009-2012 haben sich die Auskünfte von Google an staatliche Behörden und Geheimdienste verdoppelt, wie die Grafik Bild 2.4 der EFF.org zeigt.

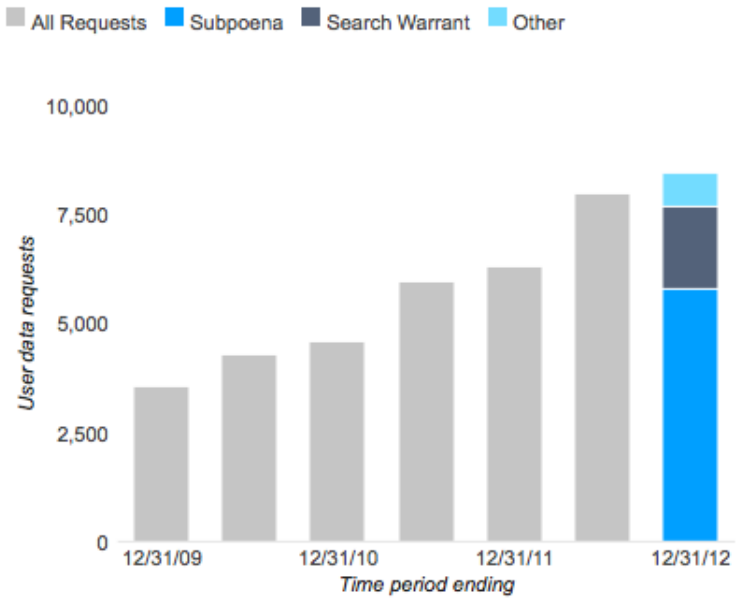


Abbildung 2.4: Steigerung der Auskünfte von Google an Behörden

Die (virtuelle) Welt ist eine "Google" - oder?

Die vernetzten Rechenzentren von Google bilden den mit Abstand größten Supercomputer der Welt. Dieser Superrechner taucht in keiner TOP500-Liste auf, es gibt kaum Daten, da das Imperium sich bemüht, diese Informationen geheim zu halten. Die Datenzentren werden von (selbstständigen?) Gesellschaften wie Exaflop LLC betrieben.

Neugierige Journalisten, Blogger und Technologieanalysten tragen laufend neues Material über diese Maschine zusammen. In den Materialsammlungen findet man 12 bedeutende Anlagen in den USA und 5 in Europa, die als wesentliche Knotenpunkte des Datenuniversums eingeschätzt werden. Weitere kleinere Rechenzentren stehen in Dublin, Paris, Mailand, Berlin, München Frankfurt und Zürich. In Council Bluffs (USA), Thailand, Malaisia und Litauen werden neue Rechenzentren gebaut, die dem Imperium zuzurechnen sind. Das größte aktuelle Bauprojekt vermuten Journalisten in Indien. (2008)

Experten schätzen, dass ca. 1 Mio. PCs in den Rechenzentren für Google laufen (Stand 2007). Alle drei Monate kommen etwa 100.000 weitere PCs hinzu. Es werden billige Standard-Komponenten verwendet, die zu Clustern zusammengefasst und global mit dem *Google File System (GFS)* vernetzt werden. Das GFS gewährleistet dreifache Redundanz bei der Datenspeicherung.

Die Kosten für diese Infrastruktur belaufen sich auf mehr als zwei Milliarden Dollar jährlich. (2007)

Die Videos von Youtube sollen für 10% des gesamten Traffics im Internet verantwortlich sein. Über den Anteil aller Dienste des Imperiums am Internet-Traffic kann man nur spekulieren.

Google dominiert unser (virtuelles) Leben.

Dabei geht es nicht um ein paar Cookies sondern um eine riesige Maschinerie.

2.1.2 Weitere Datenhändler

Die Datensammler (Facebook, Amazon, Twitter, Onlineshops...) verkaufen Informationen über Nutzer an Datenhändler (z.B. Acxiom, KaiBlue, RapLeaf...), welche die Daten anreichern, zusammenfassen und umfassende Profile den eigentlichen Endnutzern wie Kreditkartenfirmen, Personalabteilungen großer Unternehmen und Marketingabteilungen von Microsoft bis Blockbuster verkaufen.

Acxiom konnte bereits 2001, noch bevor Facebook als Datenquelle zur Verfügung stand, auf umfangreiche Datenbestände verweisen. Als das FBI die Namen der angeblichen 9/11 Attentäter veröffentlichte (von denen noch heute einige quicklebendig sind), lieferte Acxiom mehr Daten zu diesen Personen, als alle Geheimdienste zusammen - inklusive früherer und aktueller Adressen, Namen der Mitbewohner usw. Das war der Beginn einer Zusammenarbeit. Im Rahmen der Zusammenarbeit mit FBI und CIA führten die Daten von Acxiom mehrfach zu Anklagen und Abschiebungen.

Acxiom protzt damit, präzise Daten über 96% der amerikanischen Bevölkerung zu haben. In Deutschland bietet Acxiom Daten zu 44 Mio. aktiven Konsumenten an. Jeder Datensatz hat 1.500 Datenpunkte. Die Konsumenten werden in 14 Hauptgruppen unterteilt, z.B. *Alleinerziehend & statusarm, Gut situierte Midlife-Single* oder *Goldener Ruhestand & aktiv*....

Diese Hauptgruppen werden in bis zu 214 Untergruppen unterteilt nach Lifestyle-Aktivitäten (z.B. *Garten, Haustiere, Sport, Mode, Diät*...), Konsumverhalten, Milieuzuordnung (z.B. *intellektuell, statusorientiert-bürgerlich, traditionelles Arbeitermilieu, hedonistisch, konsummaterialistisch* ...) usw.

> *Sie können sich Acxiom wie eine automatisierte Fabrik vorstellen, wobei das Produkt, das wir herstellen, Daten sind.* (Aussage eines Technikers von Acxiom)

Present-Service Ullrich GmbH hat sich auf die Erkennung von Schwangerschaften und Geburten spezialisiert. Von den jährlich 650.000 Geburten in Deutschland kann die Present-Service Ullrich GmbH nach eigenen Angaben 50% erkennen und ist der Marktführer in Deutschland (Stand: 2014). Die Daten werden zusammen mit Informationen über die finanzielle Situation der Eltern für das Direktmarketing genutzt und verkauft.

Für das Direktmarketing nutzt die Firma 10.000 aktive Partner im Gesundheitswesen (Frauenärzte, Hebammen, Krankenschwestern) und verspricht den Kunden:

> *Ihre Werbebotschaft wird durch den Frauenarzt, die Hebammen bei der Geburtsvorbereitung oder Krankenschwestern bei der Geburt übergeben. Sie erzielen Customer-Touchpoints in einmalig glaubwürdiger Szenerie. So wird ihre Marke von Anfang an Teil der Familie.*

Big Data Scoring aus Estland bewertet die Kreditwürdigkeit von Personen im Auftrag von Banken und anderen Kreditgebern sowie für Kunden aus der Immobilienbrache anhand der Facebook Profile und der Aktivitäten bei anderen Social Media Sites. Das Ergebnis der Bewertung ist eine Zahl von 0...10.

RapLeaf wurde von P. Thiel gegründet, der auch die Gründung von PayPal.com finanzierte, bei Facebook maßgeblichen Einfluss hat und dessen Credo eine totale Personalisierung des Internet ist.

RapLeaf sammelt selbst Daten über die Internetnutzung und verarbeitet hinzugekaufte Daten. Die Informationen werden anhand von E-Mail Adressen zusammengefasst. Jeder kann auf der Website eine Liste von E-Mail Adressen hochladen, bezahlen und nach Zahlungseingang die Daten abrufen. Ein kleiner Auszug aus der Preisliste (Stand 2011) soll den Wert persönlicher Informationen zeigen:

- Alter, Geschlecht und Ort: 0 Cent (Lockangebot)
- Haushaltseinkommen: 1 Cent pro E-Mail-Adresse
- Ehestand: 1 Cent pro E-Mail-Adresse
- vorhandene Kinder: 1 Cent pro E-Mail-Adresse
- Wert des bewohnten Hauses: 1 Cent pro E-Mail-Adresse
- Relation von Krediten zum Vermögen: 1 Cent pro E-Mail-Adresse
- vorhandene Kreditkarten: 1 Cent pro E-Mail-Adresse

- Fahrzeuge im Haushalt: 1 Cent pro E-Mail-Adresse
- Smartphone Nutzung: 3 Cent pro E-Mail-Adresse
- Beruf und Ausbildung: 2 Cent pro E-Mail-Adresse
- Tätigkeit als Blogger: 3 Cent pro E-Mail-Adresse
- wohltätige Spenden: 3 Cent pro E-Mail-Adresse
- Präferenzen für hochwertige Marken: 3 Cent pro E-Mail-Adresse
- Präferenzen für Bücher, Zeitschriften: 3 Cent pro E-Mail-Adresse
- ...

Oracle ist eine ehemalige IT-Firma. Früher wurde Software entwickelt und neuerdings wird das Sammeln und Verknüpfen von Daten als profitabler Geschäftszweig entdeckt. Oracle wirbt mit folgenden Datenbeständen:

> *3 Milliarden Verbraucherprofile aus 700 Millionen täglichen Social-Media-Nachrichten, Daten über die Nutzung von 15 Millionen Webseiten und Einkäufe bei 1 500 Händlern.*

Das Tracking das Surfverhaltens wird mit der Auswertung des tagtäglichen Social-Media-Gedöhns und den Einkäufen in Online-Shops kombiniert.

2.2 Techniken der Datensammler

Viele Dienste im Web nutzen die Möglichkeiten, das Surfverhalten und unsere private Kommunikation zu verfolgen, zu analysieren und die gesammelten Daten zu versilbern. Die dabei entstehenden Nutzerprofile sind inzwischen sehr aussagekräftig. Es können das Einkommen, Alter, politische Orientierung, Zufriedenheit mit dem Job, Wahrscheinlichkeit einer Kreditrückzahlung, erotische Liebesbeziehungen und sexuelle Vorlieben, Schwangerschaften u.a.m. eingeschätzt werden. Ein Online-Versand von Brautkleidern möchte bspw. gezielt Frauen im Alter von 24-30 Jahren ansprechen, die verlobt sind. Ein Anbieter von hochwertiger Babyausstattung möchte gezielt finanziell gut situierte Schwangere ansprechen. Das und vieles mehr ist heute schon möglich.

Es geht aber längst nicht nur um die Einblendung von Werbung. Sarah Downey warnt [4] vor wachsenden realen Schäden durch das Online-Tracking. Die gesammelten Informationen können den Abschluss von Versicherungen und Arbeitsverträgen beeinflussen oder sie können zur Preisdiskriminierung genutzt werden. Ganz einfaches Beispiel: das US-Reiseportal Orbitz bietet z.B. Surfern mit MacOS Hotelzimmer an, die 20-30 Dollar teurer sind, als die Zimmer die Windows Nutzern angeboten werden.[5]

[4] https://heise.de/-1628313
[5] https://heise.de/-1626368

Techniken zum Tracking des Surfverhaltens

Das Surfverhalten liefert die meisten Informationen über unsere Vorlieben. Dabei werden folgende Techniken eingesetzt:

Cookies sind noch immer das am häufigsten eingesetzte Mittel, um Browser zu markieren und das Surfverhalten zu verfolgen.

Blockieren der Cookies von Drittseiten schützt nur teilweise vor dem Tracking mit Cookies. Die Datensammler haben Methoden entwickelt, um Tracking Cookies als First-Party Content zu platzieren[6]. Empirische Studien zeigen, dass es 160 Trackingdienste gibt, die mehr als 40% des Surfverhaltens verfolgen können, wenn das Setzen von Cookies für Drittseiten möglich ist. Wenn man Cookies von Drittseiten verbietet, dann können immernoch 44 Trackingdienste mehr als 40% des Surfverhaltens verfolgen. Dazu zählen:

- Google Analytics, Chartbeat.com oder AudienceScience.com schreiben die Tracking Cookies mit Javascipt als First-Party Content.
- WebTrekk nutzt DNS-Aliases, um eigene Server als Subdomain der aufgerufenen Webseite zu deklarieren und sich First-Party Status zu erschleichen.
- Yahoo! Web Analytics protzt damit, dass sie ebenfalls ihre Tracking Cookies als First-Party Content einsetzen können.

Mit diesen First-Party Cookies wird das Surfverhalten innerhalb einer Website beobachtet. Zusätzlich werden weitere Methoden eingesetzt, die eine Verknüpfung der gesammelten Daten über mehrere Webseiten hinweg ermöglichen. WebTrekk nutzt dafür Browser Fingerprinting.

Flash-Cookies werden seit 2005 verwendet, um gelöschte Tracking-Cookies wiederherzustellen. Sie sind unabhängig vom Browser und funktionieren auch, wenn man verschiedene Browser oder Browserprofile für spurenarmes Surfen und Fun-Surfen nutzt.

HTML-Wanzen (sogenannte Webbugs) sind 1x1-Pixel große transparente Bildchen, die in den HTML-Code einer Webseite eingebettet werden. Sie sind für den Nutzer unsichtbar. Beim Laden einer Webseite werden sie von einem externen Server geladen und hinterlassen Einträge in den Logdaten. Außerdem können sie Cookies transportieren.

Werbebanner und Like-Buttons können einerseits in der gleichen Weise wie HTML-Wanzen für das Tracking verwendet werden. Außerdem verrät man mit Klicks auf Werbung oder Like Buttons mehr private Informationen, als man eigentlich veröffentlichen möchte. S. Guha von Microsoft und B. Cheng sowie P. Francis vom Max-Planck-Institut für Software Systeme haben ein Paper veröffentlicht, wie man homosexuelle Männer anhand der Klicks auf Werbung erkennen kann[7]. Das Verfahren

[6] https://anonymous-proxy-servers.net/blog/index.php?/archives/377-Tracking-mit-Cookies.html

[7] http://arstechnica.com/tech-policy/news/2010/10/more-privacy-headaches-for-facebook-gay-users-outed-to-advertisers.ars

kann für verschiedene Fragestellungen angepasst werden. Die Klicks auf Facebook Like Buttons können in der gleichen Weise ausgewertet werden. Forscher der Universität Cambridge (Großbritannien) konnten bei einer Untersuchung die sexuelle Orientierung und politische Einstellung der Nutzer anhand der Klicks auf Like Buttons vorhersagen[8].

Immer häufiger nutzen Kriminelle die großen Werbenetzwerke, um mit ihrer Schadsoftware möglichst viele Rechner anzugreifen. Kriminelle kaufen passende Werbeplätze und lassen bösartige Werbebanner ausliefern oder locken die Surfer mit Anzeigen auf Malware Webseiten. Diese Angriffe werden als Malvertising bezeichnet (abgeleitet von *malicious advertising*) und nehmen derzeit stark zu. Die Sicherheitexperten von Cyphort registrierten 2015 einen Anstieg von 325% und erwarten eine Fortsetzung dieses Trends für 2016.[9]

EverCookies nutzen moderne HTML5 Techniken wie DomStorage, ETags aus dem Cache u.a. als Ersatz für Cookies, um den Surfer zu markieren und später anhand dieser Markierungen wiederzuerkennen. Der polnische Informatiker Samy Kamkar hat eine Webseite zur Demonstration von EverCookie Techniken[10] erarbeitet. 38% der populären Webseiten nutzen bereits verschiedene EverCookie Techniken (Stand: Okt. 2012).

Browser Fingerprinting nutzt verschiedene Merkmale des Browsers wie z.B. Browserversion, installierte Schriftarten, Bildschirmgröße, bevorzugte Sprachen und weitere Daten, um einen Fingerprint zu berechnen. Dieser Fingerprint ist für viele Surfer eindeutig. Das Projekt Panopticlick [11] der EFF.org zeigte, dass mehr als 80% der Surfer damit eindeutig erkennbar sind. Die Erkennungsrate stieg auf 94%, wenn Flash- oder Java-Applets zusätzlich genutzt werden konnten.

Für das Fingerprinting des Browsers werden verschiedene Techniken eingesetzt:

1. HTTP-Header: Es werden die Informationen ausgewertet, die der Browser bei jedem Aufruf sendet (Sprache, Browsername und -version, Betriebssystem und -version, unterstützte Zeichensätze, Dateitypen, Kodierungen).
2. Javascript basiert: Informationen werden per Javascript ausgelesen (installierte Schriften, Bildschirmgröße, Größe des Browserfensters).
3. Canvas basiert: In einem HTML5 Canvas Element wird ein Text gerendert und das Ergebnis via Javascript als Bild ausgelesen und ein Hash über alle Pixel als individuelles Merkmal berechnet. Das Ergebnis unterscheidet sich von Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw. Das Tracking-Verfahren wurde 2012 in dem wiss. Paper *Perfect Pixel:*

[8] https://heise.de/-1820638
[9] http://www.cyphort.com/about/news-and-events/press-releases/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks
[10] http://samy.pl/evercookie
[11] https://panopticlick.eff.org/browser-uniqueness.pdf (PDF)

Fingerprinting Fingerprinting Canvas in HTML5[12] beschrieben.

Mittels Canvas Font Fingerprinting können die installierten Schriftarten ermittelt werden. Das Verfahren wurde 2016 in dem *Open-WPM Paper* beschrieben.

4. Plug-in basiert: Informationen werden per Flash- oder Java-Plugin ausgelesen (installierte Schriftarten, Betriebssystem, Kernel Version, Multi-Monitor Setups, Bildschirmgröße).
5. Add-on basiert: Durch Seiteneffekte werden evtl. vorhandene Browser Add-ons analysiert (NoScript Whitelist, AdBlock Blacklist, fehlerhaftes User-Agent Spoofing).
6. Hardware basiert: Informationen über die Hardware des genutzten Rechners werden gesammelt (Batteriestatus, Vibrator-API, Zugriff auf Mikrofon und Webcam, Performance der Grafikhardware und spezifische Besonderheiten im Soundsystem).

Die Studien *Dusting the Web for Fingerprinters*[13] (2013) und *The web never forgets*[14] (2014) der KU Leuven (Belgien) haben nachgewiesen, das Fingerprinting bereits für das Tracking genutzt wird:

- *Bluecava* nutzt ausschließlich Browser Fingerprinting und protzt mit 30% besseren Ergebnissen als Cookie-basierte Techniken.[15]
- *Zanox.com* nutzt den Fingerprint des Browsers, wenn Cookies gelöscht oder per Browser-Einstellung blockiert werden.[16]
- *WebTrekk* berechnet einen Fingerprint auf Grundlage von Geolocation anhand der IP-Adresse, Bildschirmgröße und Farbtiefe des Monitors, innere Größe des Browserfensters, bevorzugte Sprache, User-Agent des Browsers, Version des Betriebssystems sowie Einstellungen für Java, Javascript und Cookies (AN/AUS).[17]
- *Multicounter* nutzt den Fingerprint zusätzlich zu Cookies oder Ever-Cookies zur Verbesserung der Erkennungsraten.[18]
- *Piano Media* verwendet Flash-basiertes Fingerprinting, um Paywall Restriktionen für Online Medien durchzusetzen.
- *Anonymizer Inc.* verwendet Browser Fingerprinting auf sämtlichen Webseiten, verschweigt es aber im Privacy Statement. (Eine seltsame Auffassung für jemanden, der Anonymität verkaufen will.)
- *Yahoo! Web Analytics* nutzt Javascript Tracking Code, wenn Cookies blockiert werden.
- Canvas Fingerprinting wird u.a. von den Trackindiensten *doubleverify.com, lijit.com* und *alicdn.com* genutzt. Auf 14.371 Webseiten wurden Trackingscripte mit Canvas Fingerprinting nachgewiesen. (Stand: 2016)

[12] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[13] http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[14] https://securehomes.esat.kuleuven.be/ gacar/persistent/the_web_never_forgets.pdf
[15] http://www.bluecava.com/visitor-insight-campaign-measurement
[16] http://blog.zanox.com/de/zanox/2013/09/11/zanox-stellt-tpv-fingerprint-tracking-vor/
[17] http://www.webtrekk.com/de/index/datenschutzerklaerung.html
[18] http://www.multicounter.de/features.html

- AudioContext Fingerprinting wurde bei drei Trackingdiensten nachgewiesen, die jedoch nur einen sehr geringe Reichweite haben und nur auf wenigen Webseiten eingebunden sind.

Da Browser Fingerprinting keine Markierungen einsetzt, die man löschen könnte, ist eine Verteidigung besonders schwer realisierbar. Wichtigste Verteidigunsmaßnahmen sind das Blockieren von Javascript (vor allem für Drittseiten), blockieren von Flash und die Nutzung von AdBlock, um Tracking-Scripte im First-Party Kontext zu blockieren.

Keystroke Biometrics verwendet das Schreibverhalten der Nutzer auf der Tastatur als Identifizierungsmerkmal. Der HTML5 Standard definiert eine API, um auf Tastaturereignisse reagieren zu können. In Firefox 38.0 wurden erste Teile der API standardmäßig aktiviert. In Kombination mit hochgenauen Timern können Webapplikationen das Schreibverhalten der Surfer in Webformularen analysieren und als biometrischen Login verwenden (z.B. von der Firma KeyTrac angeboten) oder als Trackingfeature.

Mit Windows 10 hat Microsoft begonnen, das Schreibverhalten der Anwender im Hintergrund durch das Betriebssystem analysieren zu lassen und die erstellten biometrischen Profile an die Firma BehavioSec zu senden, die mit der DARPA und Microsoft kooperiert. Laut Eigenwerbung kann BehavioSec 99% der Nutzer korrekt erkennen. Die dabei entstehenden umfangreiche Sammlung der biometrischen Profile kann zukünftig zum Tracking und zur Deanonymisierung genutzt werden.

Für die Auswertung werden nicht nur die Informationen zur besuchten Webseite genutzt. Besonders aussagekräftig sind z.B. die Klicks auf Werbung.

Tracking von E-Mail Newslettern

Die Markierung von E-Mail Newslettern ist weit verbreitet. Es geht dabei darum, das Öffnen der E-Mails zu beobachten und die Klicks auf Links in den Newslettern zu verfolgen.

- Wie beim Tracking des Surfverhaltens werden kleine 1x1 Pixel große Bildchen in die E-Mail eingebettet, die beim Lesen im HTML-Format von einem externen Server geladen werden. Durch eine individuelle, nutzerspezifische URL kann die Wanze eindeutig einer E-Mail Adresse zugeordnet werden. Ein Beispiel aus dem E-Mail Newsletter von Paysafecard, das einen externen Trackingservice nutzt:

  ```
  <IMG src="http://links.mkt3907.com/open/log/43.../1/0">
  ```

  Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

  ```
  <IMG src="http://mail.easyjet.com/log/bEAS001/mH9..."
       height=0 width=0 border=0>
  ```

Bei kommerziellen E-Mail Newslettern kann man fast sicher davon ausgehen, dass sie Wanzen enthalten. Ich habe diese Trackingelemente in so gut wie allen kommerziellen Newslettern von *PayPal.com, Easyjet, AirBerlin, Paysafecard, UKash* usw. gefunden. Es wird aber nicht nur im kommerziellen Bereich verwendet. Die CDU Brandenburg markierte ihre Newsletter über einen längeren Zeitraum, um zu überprüfen, wann und wo sie gelesen wurden. *ACCESS Now* und *Abgeordnetenwatch* sind weitere Beispiele.

- Neben kleinen Bildern können weitere HTML-Elemente wie CSS Stylesheets, Media Dateien oder Link Prefetching in einer E-Mail genutzt werden. Der E-Mail Privacy Test[19] zeigt eine umfangreiche Liste. Diese Elemente werden in der Praxis aber kaum genutzt.

- Die Links in den E-Mails führen oft nicht direkt zum Ziel. Sie werden über einen Trackingservice geleitet, der jeden Klick individuell für jede Empfängeradresse protokolliert und danach zur richtigen Seite weiterleitet. Als Bespiel soll ein Link aus dem Paysafecard Newsletter dienen, der zu einem Gewinnspiel auf der Paysafecard Webseite führen soll:

```
<a href="http://links.mkt3907.com/ctt?kn=28&ms=3N...">
Gewinne Preise im Wert von 10.000 Euro</a>
```

Als Schutzmaßnahme gegen dieses Tracking sollte man Mails als Text lesen.

Tracking von Dokumenten (PDF, Word usw.)

Die Firma ReadNotify bietet beispielweise einen Service, der Word-Dokumente und PDF-Dateien mit speziellen unsichtbaren Elementen versieht. Diese werden beim Öffnen des Dokumentes vom Server der Firma nachgeladen und erlauben somit eine Kontrolle, wer wann welches Dokument öffnet. Via Geo-Location ermittelt ReadNotify auch den ungefähren Standort des Lesers. Aus der Werbung von ReadNotify: [20]

> *We not only let you know when your document or PDF was opened, but we will also endeavor to let you know:*
>
> - *Date, time, location, ISP, etc regarding each reading*
> - *Recipient / reader details*
> - *When applicable, details showing when your document was Printed out (on paper) or Saved (a copy made to disk)*
> - *Details on whether or not it was forwarded (and where possible; to whom)*
> - *Which pages of your PDF were read*
> - *Length of time read*
> - *How many times it was opened and re-opened (with optional instant notifications each time)*

[19] https://emailprivacytester.com/
[20] https://ssl1.readnotify.com/readnotify/pmdoctrack.asp

2.3 Tendenzen auf dem Gebiet des Tracking

Obwohl 80% der Internetnutzer das Tracking des Surfverhaltens ablehnen, wird es stetig weiter ausgebaut. Dabei wird es sowohl technisch durch die großen Datensammler immer weiter ausgebaut und durch politische Entscheidungen werden Datensammlungen erleichtert.

1. Mehr Trackingelemente werden auf den Webseiten eingesetzt. Das Projekt Web Privacy Census der University of California verfolgt seit mehreren Jahren die Entwicklung und dokumentiert einen stetigen Anstieg von Trackingelementen bei den meistbesuchten Webseiten (Top-100, Top-1000 und Top-25.000). Als Beispiel soll die Anzahl der Cookies dienen, die beim Besuch der 100 populärsten Webseiten gesetzt werden (ohne Login, nur beim Betrachten der Webseiten):

	Anzahl der Cookies
2009	3.602
2011	5.675
2012	6.485

2. Das Projekt registriert eine überproportionale Zunahme schwer blockierbarer Trackingfeatures (EverCookies). Immer mehr Webseiten verwenden HTML5 DomStorage, IE_userdata oder ETags aus dem Cache für die Verfolgung des Surfverhaltens. Für die meistbesuchten Webseiten wurden folgende Zahlen zur Nutzung von EverCookies ermittelt:

	Nutzung von EverCookies
2011	19% der Webseiten
2012 (Mai)	34% der Webseiten
2012 (Okt.)	38% der Webseiten

3. Flash-Cookies (LSOs) werden seltener eingesetzt. Diese Technik befindet sich auf dem absteigenden Ast. Im Oktober 2012 setzten nur noch 11% der populären Webseiten Flash-Cookies ein. Dabei handelt es sich überwiegend um Webseiten mit Flash-Videos. *Youporn.com* speichert persönliche Preferenzen beispielsweise in Flash-Cookies.

4. Durch den Aufkauf kleinerer Anbieter durch die Großen der Branche erfolgt eine Marktbereinigung. Es bilden sich sogenannte Tracking-Familien, die die Daten untereinander austauschen und somit eine große Reichweite bei der Beobachtung des Surfverhaltens haben. Die größten Tracking-Familien sind:

   (a) Die Google-Familie ist unangefochten die Nummer Eins. 44% der weltweiten Umsätze in der Onlinewerbung werden durch diese Gruppe erzielt. Das Google Imperium hat in den letzten Jahren die Firmen *YouTube, DoubleClick mit falkad.net, FeedBurner, Springs, Adscape, AdMob, Teracent, Invite Media, Admeld, Adelphic, Wildfire Interactive* u.a.m. aufgekauft. Nach dem OpenWPM Report von 2016 gehören die TOP5 Tracking Dienste alle zur Google Familie und von den TOP20 Tracking Diensten gehören 12 zum Google Imperium.

Die folgende Tabelle zeigt, wie das Google Imperium dadurch seine Präsenz auf den 1000 populärsten Webseiten in den letzten Jahren ausbauen konnte:

	Trackingelemente der Google-Familie
2005	auf 7% der Webseiten
2006	auf 16% der Webseiten
2008	auf 55% der Webseiten
2009	auf 80% der Webseiten
2012	auf 97% der Webseiten

(b) Auf den Plätzen 2 und 3 folgen Facebook und Twitter, die vor allem mit Like Buttons und ähnlichem Social Media Kram tracken und 2016 eine Abdeckung von mehr 10% der 1-Million-Top-Sites erreichten. Die Kooperation von Facebook mit den eigenständigen Trackingdiensten BlueKai und Epsilon ist dabei noch nicht enthalten.

(c) Auf den folgenden Plätzen liegen etwas abgeschlagen die Tracking-Familien von Microsoft (u.a. mit den Trackingdiensten *atdmt.com, adbureau.com, aquantive.com*), die Yahoo! Familie (mit den Trackingdiensten *adrevolver, yieldmanager, overture*), die AOL-Familie (mit *adsonar.com, tacoda.net, advertising.com*) und die Oracle Data Cloud (mit *BlueKai, Datalogix, AddThis*) mit einem Marktanteil von jeweils 3-8%.

5. Die Beobachtung des Surfverhaltens und der Online-Einkäufe liefert nur ein unvollständiges Bild unserer Interessen. Durch Einbeziehung von Daten aus dem realen Leben sollen die Profile verbessert werden.

   - Im Februar 2013 hat Facebook eine Kooperation mit den Datenhändlern *Axciom* und *Datalogix* bekannt gegeben. Diese Firmen werten umfangreiche Daten aus der realen Welt aus (Kreditkartenzahlungen, Rabattkarten usw.). Damit sollen die Werbeeinblendungen bei Facebook individueller und zielgerichteter auf die Interessen der Mitglieder zugeschnitten werden.
   - PayPal.com will sein Bezahlsystem auch offline in der realen Welt anbieten und verspricht den teilnehmenden Geschäften, dass sie mehr über die Vorlieben ihrer Kunden erfahren werden. Natürlich wird auch PayPal.com mehr über die realen Interessen der Kunden erfahren.
   - Patentanmeldungen von Google und Firmen Akquisitionen zeigen, dass das Imperium zukünftig auch Daten in der realen welt sammeln möchte. Anfang 2014 kaufte Google z.B. mit Nest einen Hersteller von Thermostaten und Rauchmeldern für 3,1 Milliarden Dollar. Die Thermostate von Nest sind in Millionen Haushalten eingebaut und mit Temperatur-, Helligkeits- sowie Luftfeuchtigkeitssensoren ausgerüstet, die via Internet ausgelesen werden können.

     > *Dank Nests eingebauter Sensoren weiß Google jetzt, wann Sie zuhause sind, in welchem Raum Sie sich aufhalten und dank der Feuchtigkeitssensoren im Schlafzimmer auch, wie oft, wie lange und wie leidenschaftlich Sie Sex haben.* (M. Morgenroth)

6. Alle Datensammlungen wecken natürlich Begehrlichkeiten bei den Geheimdiensten und Strafverfolgern. Leider ist wenig konkretes darüber bekannt. Bei der Anhörung des US Senate Commerce Committee zu den Problemen von Online-Tracking im Juni 2012 sagte B. Liodice als Vertreter der Werbeindustrie, dass das Tracking des Surfverhaltens der Internetnutzer für die Sicherheit der USA wichtig und notwendig ist.

   Die EFF.org kommentierte:

   > *In yesterday's Senate hearing, we heard the advertising industry admit that their near-ubiquitous online tracking program is being used for issues that are the purview of law enforcement.*

   Durch die Snowden-Dokumente wurden konkrete Beispiele bekannt.[21]

   - Die NSA beobachtet den Datenverkehr und nutzt z.B. die Tracking Cookies der Datensammler zur Beobachtung der Surfer und zur Identifikation von Targets, deren Computer mit Trojanern infiziert werden sollen. Insbesondere Das PREF Cookie von Google wird von der NSA gern genutzt.
   - Außerdem nutzt die NSA die Standortinformationen, die von Smartphone Apps an Datensammler (Service Provider, Entwickler) gesendet werden, um Personen zu lokalisieren (HAPPYFOOT).

7. Von der Politik ist wenig Unterstützung für Datenschutz zu erwarten. Wie unsere Bundeskanzlerin mehrfach betont hat, leben wir in einer *marktkonformen Demokratie*. Die Demokratie hat sich also marktkonform anzupassen und in erster Linie den sogenannten Wertschöpfungen nicht im Wege zu stehen. Neben den *Finanzprodukten* aus dem Bankensektor (die nichts weiter sind als Umverteilung von Geld) gilt jetzt auch das Sammeln und Auswerten von privaten Daten als eine Art Wertschöpfung, die neue Produkte ermöglicht, über die die Kunden mehrheitlich erfreut sein sollen.

   Auf dem Wirtschaftstag 2015 hat Bundeskanzlerin Merkel sich gegen den Datenschutz und für diese neue Art der Wertschöpfung positioniert. Ihrer Meinung nach sind Daten der bedeutenste Rohstoff dieses Jahrhunderts und die Ausbeutung dieses Rohstoffes sollte nicht durch strenge Datenschutzrichtlinien beeinträchtigt werden.[22]

   > *Die eigentliche Musik wird stattfinden jetzt in der Debatte um die Datenschutzgrundverordnung, um das Big Data Management, und da müssen wir aufpassen, dass wir in Europa nicht ein klein wenig schizophren sind. Wir haben das schöne Safe Harbor Abkommen mit den Vereinigten Staaten von Amerika, das heißt, es können alle Daten aus Europa nach Amerika geschickt werden und dort zu neuen Produkten verarbeitet werden, und der europäische Kunde ist froh, mit diesen Produkten dann hantieren zu können. Wir müssen es schaffen,*

[21] https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons
[22] https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/

> *ein solches Big Data Management zu machen, dass Wertschöpfung hier auch in Europa stattfinden kann.*

Auf dem IT-Gipfel 2016 in Saarbrücken hat Bundeskanzlerin Merkel diese Linie der Bundesregierung nochmal bekräftigt und sich vom Grundprinzip der Datensparsamkeit als Leitlinie verabschiedet. Sie sagte wörtlich:

> *Denn das Prinzip der Datensparsamkeit, wie wir es vor vielen Jahren hatten, kann heute nicht die generelle Leitschnur sein für die Entwicklung neuer Produkte.*

Wir werden also zukünftig mehr auf Selbstschutz angewiesen sein. Dieser Selbstschutz könnte zukünftig aber schwieriger werden. In der Auseinandersetzung zwischen Werbewirtschaft und AdBlockern stellen sich Bundestag und Bundesrat auf die Seite der Werbewirtschaft. In dem *Abschlussbericht der Bund-Länder-Kommission zur Medienkonvergenz* vom Juni 2016 befasst sich ein eigenes Kapitel damit, wie sich Medien gegen den zunehmenden Einsatz von Werbeblockern schützen können. Ein gesetzliches Verbot von Werbeblockern wird diskutiert:

> *. . . eine zeitnahe Prüfung durch Bund und Länder klären, ob im Hinblick auf die wirtschaftlichen Auswirkungen und damit verbundenen medienpolitischen Risiken gegebenenfalls eine gesetzliche Flankierung geboten ist.*

Unklar ist, wie ein solches Verbot umgesetzt und durchgesetzt werden kann. Nach Ansicht der Interessenvertreter der Werbeindustrie gibt es aber *einen rechts- und medienpolitischen Bedarf für ein gesetzliches Verbot von Ad-Blockern* und sie werden darin von führenden Regierungsmitgliedern unterstützt.

8. Der *Point of no Return* ist längst überschritten. Am 06. Okt. 2015 hat der Europäische Gerichtshof (EuGH) das Safe Habour Abkommen für ungültig erklärt[23], dass bisher den Datentransfer in die USA erlaubte. Die Verquickung von Facebook mit den US-Geheimdiensten im Rahmen von PRISM spielte eine wesentliche Rolle bei der Urteilsfindung.

   Google und Facebook haben daraufhin erklärt, dass sie auch ohne Safe Habour Abkommen so weitermachen wie bisher und die Daten europäischer Nutzer in die USA transferieren und dort verarbeiten werden[24]. Sie sehen die EU-Standardvertragsklauseln nach Artikel 26, Absatz 2 der EU-Datenschutzrichtlinie von 1995 (EC95/46) als ausreichende Grundlage an. In dieser Ansicht werden sie von der EU-Kommision unterstützt.[25]

   Meiner Meinung nach haben die europäischen Regierungen und die EU keine andere Möglichkeit, als vor der Marktmacht der US-Konzerne zu

[23] https://www.heise.de/tp/artikel/46/46186/1.html
[24] http://www.golem.de/news/safe-harbor-urteil-google-und-microsoft-suchen-neue-wege-des-datentransfers-1510-116945.html
[25] http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm

kapitulieren. Wenn man Google & Co. das Sammeln von Daten über europäische Nutzer verbieten würde, dann könnten die US-Konzerne im Gegenzug den Zugriff auf ihre Dienste für europäische Nutzer sperren, da sie nicht mehr mit ihren Daten zur Finanzierung der Dienste beitragen. (Im kleineren Maßstab hat es Google beim Leistungsschutzrecht schon einmal demonstriert.)

Die Mehrheit der europäischen Nutzer würde es nicht akzeptieren, auf Facebook, Google, Youporn und Twitter, Microsoft Windows, Apples MacOS und iPhones sowie Android Smartphones usw. verzichten zu müssen. DAS wäre ein hinreichender Grund für einen Aufstand. Somit muss die EU-Kommission dem gemeinsamen Druck der US-Regierung und der US-Firmen nachgeben und ein Konstrukt finden, dass das Sammeln von Daten zur Finanzierung der Services und zur Auswertung durch die US-Geheimdienste (z.B. im Rahmen von PRISM) weiterhin erlaubt.

Dass das neue *Privacy Shield* Abkommen (der Nachfolger von *Safe Habour*) eine Kapitulation der EU beim Thema Datenschutz gleichkommt, konnte man erwarten und ist keine Überraschung.

9. Die zukünftige Entwicklung könnte durch folgende Eckpunkte gekennzeichnet sein:

   - Weitere Ausweitung des Marktes auf die zwischenmenschliche Kommunikation
   - Vereinzelung der Individuen durch Pseudogemeinschaften in der virtuellen Welt
   - Kontrolle aller digitalen Aktivitäten durch die *smarte Diktatur*

2.4 Crypto War 3.0

Im Januar 2015 hat der britische Premierminster Cameron den **crypto war 3.0** mit der Forderung eröffnet, dass jede Kommunikation für Geheimdienste einsehbar sein muss. Weitere Politiker wie Obama, unser Innenminister de Maizière oder der australische Justizminister Keenan assistierten. Als hinreichender Grund wird der allgegenwärtige TERRORISMUS kolportiert, der unsere demokratischen Werte bedroht.

Ein generelles Verbot starker Kryptografie wird nicht ernsthaft diskutiert. Es wäre nicht durchsetzbar und eine kommerzielle Nutzung des Internets wäre praktisch tot. Damit sind nicht Googles Werbeeinnahmen gemeint sondern industrielle Anwendungen, mit den denen richtig viel Geld umgesetzt wird (z.B. im Bereich Banken, Börsen usw.).

Ein Schwerpunkt der aktuellen Angriffe auf Verschlüsselung richtet sich gegen Messenger Apps für Smartphones. Dabei sind zwei Angriffs-Muster erkennbar:

Forderung nach Backdoors: Diese Strategie ist nicht neu und wurde schon mehrfach gegen Kommunikationsdienste erfolgreich eingesetzt, sobald diese Dienste eine nennenswerte Popularität erreichten.

- Skype wurde 2005 durch Anwendung des CALEA Act. gezwungen, Schnittstellen für die Überwachung bereitzustellen. Diese Überwachung wurde ständig weiter ausgebaut und heute liest Microsoft als Betreiber des Dienstes ungeniert mit.
- Blackberry wurde in Kanada, in Indien und in anderen Ländern gezwungen, den Behörden die Schlüssel für die Entschlüsselung zur Verfügung zu stellen.

Aktuelle, konkrete Forderungen des FBI richten sich an die großen Kommunikationsdienstleister wie Google, Apple, Microsoft, Facebook, Whatsapp... Sie sollen freiwillig die Möglichkeiten implementieren, um staatliche US-Behörden auf Anforderung die Inhalte der Kommunikation unverschlüsselt liefern zu können. Gesetzliche Vorgaben sind im Moment (nach den Snowden-Leaks?) in der EU und den USA nicht populär.

Gelegentlich versucht das FBI, seinen Wünschen mit der Terrorismus-Keule in einem Präzedenzfall mehr Nachdruck zu verleihen (siehe: Apple vs. FBI). Grundsätzlich sind alle US-Firmen zur stillen Kooperation bereit, auch Apple. Aber eine offizielle Hintertür für ihre Krypto wollen die US-Firmen aus PR-Gründen vermeiden.

In Russland wird gegenwärtig die Forderung nach gesetzlich vorgeschriebenen Hintertüren in der Verschlüsselung bei Messenger Apps am konsequentesten umgesetzt. Ein neues Anti-Terror Gesetz soll u.a. alle Anbieter von Messaging Diensten zwingen, dem Geheimdienst FSB die Möglichkeit zur Entschlüsselung der Kommunikation zu geben. Außerdem sollen die Inhalte der Kommunikation für 6 Monate und die Metadaten für 3 Jahre gespeichert werden.

Wenn man eine Verschlüsselung entwickeln will, die gegen staatliche Angriffe robust sein soll, dann kann man das russische Gesetz als Referenz-Angriff nehmen.

Staatliches Hacking und Einsatz von Trojanern Da Hintertüren in der Verschlüsselung von Kommunikation zur Zeit in der EU und den USA nicht populär sind, versucht man es mehr mit staatlichen Hackerangriffen, die gesetzlich legitimiert und personell besser ausgestattet werden.

- In Deutschland nimmt die im Nov. 2015 angekündigte Bundes-Hacker-Behörde zur Unterstützung von Geheimdiensten und Strafverfolgung beim Brechen von Verschlüsselung langsam Gestalt an. Die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (Zitis) soll 2017 mit 60 Mitarbeitern einsatzbereit sein und dann

schrittweise auf 400 Mitarbeiter ausgebaut werden.[26]

Neben Angriffen auf die Verschlüsselung soll diese Behörde technische Werkzeuge entwickeln, mit denen der Computer einer Zielperson infiltriert werden kann (sogenannte Bundestrojaner).

- In den USA soll *Rule 41 of the US Federal Rules of Criminal Procedure* ab Dez. 2016 das staatliche Hacken von Tor- und VPN-Nutzern für das FBI massiv erleichtern, unabhägig davon, in welchem Land die Tor-Nutzer sich befinden.[27]

2.5 Fake News Debatte

Ende Nov. 2016 hat Bundeskanzlerin Merkel das Thema Fake News als Bedrohung für die kommenden Wahlen deklariert. Alternative Medien und Diskussionen in abgeschotteten Facebook Gruppen sollen eine Gefahr sein, die die Informationshoheit der etablierten Mainstream Medien in Frage stellen und mit Falschmeldungen untergraben.

Mir fallen spontan folgende Fake News ein:

- Fake: *Irakische Soldaten haben beim Überfall auf Kuweit frügebohrene Säuglinge aus den Brutkästen gerissen und auf dem Boden des Krankenhauses liegengelassen, wo die Säuglinge starben.* (Brutkastenlüge, vom damaligen US-Präsidenten George H. W. Bush und von Menschenrechtsorganisationen vielfach zitiert.)

  Wahr: Die *Brutkastenlüge* wurde völlig faktenfrei von der PR-Agentur Hill & Knowlton im Auftrag der kuwaitischen Exil-Regierung erfunden. Die *Krankenschwester*, die als Zeugin aussagte, war die Tochter des des kuwaitischen Botschafters in den USA.

- Fake: *Der Irak hat Massenvernichtungswaffen! Insbesondere verfügt Dikator Saddam Hussein über mobile Biowaffen Labore, die auf Tiefladern montiert sind und hochbeweglich.* (US-Verteidigungsminister Rumsfeld und US-Außenminister C. Powell)

  Wahr: Alles komplett erlogen, die Story wurde unter Mithilfe des BND produziert und in der UNO als als hinreichenden Grund für einen Überfall auf den Irak präsentiert. Nach dem Bericht der Iraq Survey Group (ISG) besaß der Irak 2003 keine ABC-Waffen.[28]

- Nochmal als Fake aufgewärmt: 2014 wird behauptes, bei den Chemiewaffen des IS soll es sich um die damals nicht gefundenen irakischen Massenvernichtungswaffen handeln, die jetzt dem Islamischen Staat in

[26] https://netzpolitik.org/2016/bundesregierung-will-entschluesselungsbehoerde-schaffen
[27] https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government
[28] http://www.faz.net/aktuell/politik/ausland/irak-krieg-keine-massenvernichtungswaffen-1175499.html

die Hände gefallen sind.[29]

Der investigative Journalist Seymour Hersh schreibt, dass die Chemiewaffen in den Händen der Terroristen des IS aus Libyen stammen und von dort mit Zustimmung der Ex-US-Außenministerin H. Clinton über die Türkei nach Syrien gebracht wurden.[30]

- Fake: *Whistleblower Edward Snowden könnte ein russischer Spion sein.* (G. Maaßen, Chef des BfV) oder *Snowden ist ein Russen-Agent.* (J. R. Schindler)

  Wahr: E. Snowden ist gegen seinen Willen in Russland gestrandet, weil der US-Geheimdienst CIA unprofessional gearbeitet hat und unfähig war, Snowden festzusetzen. Russland hat ihm in auswegloser Situation Asyl gewährt.

- Fake: *Es wird ein No-Spy-Abkommen mit den USA geben.* (Bundeskanzlerin A. Merkel, Innenminister H.-P. Friedrich, Kanzleramtsminister R. Pofalla, Regierungssprecher S. Seibert)

  Wahr: Nach Berichten von NDR und WDR war der Bundesregierung bereits 2013 bekannt, dass die US-Regierung nie ein No-Spy-Abkommen angeboten hatte und zu einem solchen Abkommen auch keine Zustimmung von der US-Regierung zu erwarten war. Man brauchte aber etwas Gegengift zu den Snowden-Enthüllungen.

- Fake: *Die AfD ist eine rechts-populistische Partei der Geringverdiener und ein Sammelbecken für die sozial Abgehängten der Gesellschaft.*

  Wahr: Die AfD ist eine konservative Partei, deren Mitglieder überwiegend zur Mittelschicht gehören. Der Anteil der Geringverdiener (unter 2.000 Euro Netto) unter den AfD-Anhängern entspricht mit 27% der Anhängerschaft der CDU (28% Geringverdiener) und ist geringer als bei SPD (32%) und Linke (37%).[31]

- Fake: *Steckt Russland hinter der Attacke auf Telekom-Router?* Bundeskanzlerin Merkel und BND Präsident Kahl warnen angesichts des Telekom Hack vor Angriffen aus Russland, denn *nach den Erkenntnissen des BND wollen russische Hacker die Demokratie zerstören!*

  Wahr: Es gab KEINEN Angriff auf die Telekom, der Ausfall der Telekom Router war nur ein Kolateralschaden. Die kriminellen Betreiber des Mirai Botnetzes wollten Zyxel-Router angreifen, die der irische Provider Eir an seine Kunden verteilte und die einen Security Bug im TR-069 Interface haben. Die Telekom Router hatten sich bei den automatisierten Tests des Mirai Botnetzes auf Verwundbarkeit selbst abgeschaltet.[32]

[29] http://www.zeit.de/politik/ausland/2014-10/chemiewaffen-irak-armee
[30] http://www.strategic-culture.org/news/2016/04/28/seymour-hersh-hillary-approved-sending-libya-sarin-syrian-rebels.html
[31] http://www.zeit.de/politik/deutschland/2016-11/afd-waehler-geringverdiener-spd-die-linke-forsa-umfrage
[32] https://heise.de/-3520212

- Fake: Die deutschen Geheimdienste machen russische Hacker für die Wikileaks-Enthüllungen zum NSA-Ausschuss verantwortlich. Einige Politiker warnen in diesem Zusammenhang vor Einflussversuchen auf die Bundestagswahl 2017.[33]

  Wahr: Die mit den Ermittlungen beauftragten Sicherheitsbehörden des Bundes und die Staatsanwaltschaft sind überzeugt, dass es keine Hacker waren und dass die Quelle im Bundestag sitzt. Sie ermitteln wegen Verletzung des Dienstgeheimnisses.[34]

- Zu personenbezogenen Fake News könnte man noch erwähnen, dass der GCHQ Rufmord im Internet gezielt plant und umsetzt (wahrscheinlich nicht nur der GCHQ). Zu den konkreten Methoden der JTRIG (Joint Threat Research Intelligence Group) gehört es, Personen mit Sexangeboten in kompromittierende Situationen zu locken, Falschinformationen unter ihrem Namen im Netz zu publizieren oder Mails an Freunde und Kollegen unter ihrer Identität zu verschicken. Eine weitere Taktik besteht darin, sich in Foren als Opfer einer Person auszugeben, die man schädigen möchte.

Das alles war nie ein Problem, aber wenn das Wahlergebnis 2017 möglicherweise nicht mehr den Erwartungen der politischen Elite entspricht, dann ist es etwas gaaanz anderes?

Der beste Schutz gegen Fake News und Propagandalügen ist **Medienkompetenz**. Übereilte gesetzliche Regelungen oder Privatisierung der Wahrheitsfindung durch Unternehmen wie Facebook oder Twitter sind im Spannungsfeld von freier Meinungsäußerung keine Lösung.

Das Ergebnis der Wahlen in den USA, der Brexit und kommende Votes sind NICHT durch ein paar Fake News manipuliert und wurden auch nicht von bösen russischen Hackern herbei geführt, die die Demokratie zerstören wollen. Prof. S. Hawkins hat meiner Meinung nach die beste brauchbare Anlayse zur aktuellen Situation geschrieben:

> *Whatever we might think about the decision by the British electorate to reject membership of the European Union and by the American public to embrace Donald Trump as their next president, there is no doubt in the minds of commentators that* ***this was a cry of anger by people who felt they had been abandoned by their leaders****.*
> ...
> *So taken together we are living in a world of widening, not diminishing, financial inequality, in which many people can see not just their standard of living, but their ability to earn a living at all, disappearing. It is no wonder then that* ***they are searching for a new deal****, which Trump and Brexit might have appeared to represent.*

[33] http://www.faz.net/aktuell/politik/inland/wikileaks-sicherheitskreise-russland-hackte-geheime-bundestagsakten-14568558.html

[34] http://www.golem.de/news/nsa-ausschuss-wikileaks-koennte-bundestagsquelle-enttarnt-haben-1612-124857.html

Die Menschen fühlen sich im Stich gelassen von einer politischen Elite, die es sich selbst bequem gemacht hat. Sie wollen eine Veränderung, denn bei jeder Veränderung gibt es eine Chance auf Verbesserung im Gegensatz zur *Weiter so...* Politik von A. Merkel. Die Suche nach Veränderung eröffnet nicht nur neue Chancen sondern birgt auch Gefahren.

2.6 Geotagging

Geotagging ist *the next big thing* unter den Angriffen auf die Privatsphäre. Es geht um die Frage, wo wir etwas tun oder getan haben und welche Bewegungsmuster erkennbar sind.

1. **Standortdaten** sind die wertvollsten Informationen für die Werbewirtschaft, um zukünftig den Markt zu vergrößern. Ein Online-Versand von Brautkleidern richtet seine Werbung an Frauen zwischen 24-30 Jahren, die verlobt sind. Ein Ladengeschäft stellt zusätzlich die Bedingung, dass sie sich häufig im Umkreis von xx aufhalten. Lokalisierte Werbung ist ein Markt, der durch die Verbreitung von Smartphones stark wächst.

2. Die Analyse des Soziales Umfeldes ist mit den Standortdaten ebenfalls möglich. Die Summe aller Standortdaten ist mehr, als die Anhäufung der Standorte von Person A, B und C. Wie die Studie *Inferring social ties from geografic coinsidences*[35] zeigt, ermögliche diese Sammlung detaillierte Informationen über das soziale Umfeld, auch wenn man bei Facebook nicht befreundet ist. Die Standortdaten der Smartphones verraten, mit wem man regelmäßig ein Bier trinkt, mit wem man ins Bett steigt, ob man an Pegida Demonstrationen teilnimmt oder sich in Antifa Zirkeln trifft und vieles mehr.

3. Mit den Geofenching Datensammlungen ist eine einfache **Überwachung** und **Einschüchterung** möglich. In der Ukraine wurden diese Daten bereits im Jan. 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:

   > *Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.*

   Die Firma Dataminr bietet Kunden via API Zugriff auf die Twitter Postings und wirbt in einem Flyer am Beispiel eines Studentenprotestes in Südafrika damit, wie man das neue Geospatial Analyse Tool Bild 2.5 zum Monitoring von politischen Demonstrationen nutzen kann.

4. Die **Bewegungsanalyse** ermöglicht Aussagen über sehr private Details. Man kann z.B. durch die Analyse der Handybewegungen erkennen, ob jemand als Geschäftsreisender häufig unterwegs ist, ob man ein festes Arbeitsverhältnis hat, für welche Firma man tätig ist oder ob man arbeitslos ist. Die Firma Sense Networks ist ein Vorreiter auf dem Gebiet der

[35] http://www.pnas.org/content/107/52/22436.short

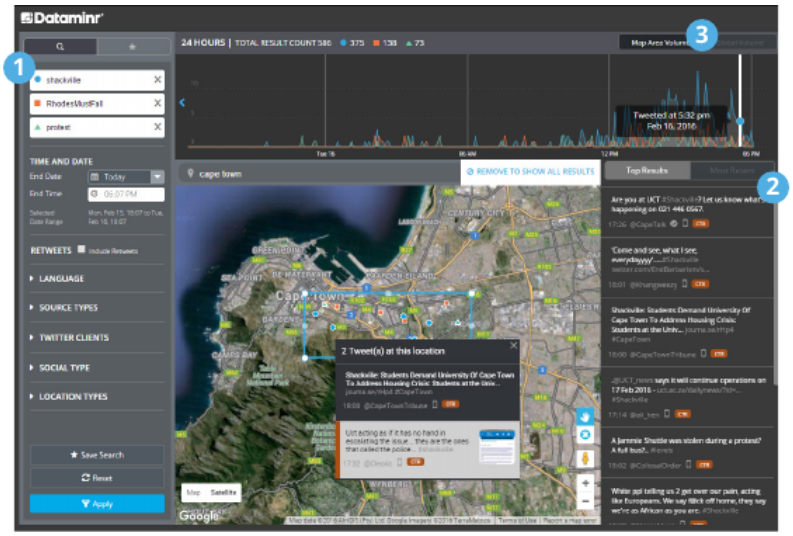


Abbildung 2.5: Auswertung der Twitter Postings eines Studentenprotestes in Südafrika aufgrund der Geoloaction der Postings

Bewegungsanalyse. Im Interview mit *Technology Review* beschreibt Greg Skibiski seine Vision:

> *Es entsteht ein fast vollständiges Modell. Mit der Beobachtung dieser Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen* [36].

Das Magazin Wired berichtete im Danger Room (Oktober 2011), dass das FBI Smartphones bereits seit Jahren mit der Zielstellung der "Durchleuchtung der Gesellschaft" trackt. Muslimische Communities werden systematisch analysiert, ohne dass die betroffenen Personen im Verdacht einer Straftat stehen. Das Geotracking von GPS-fähigen Smartphones und GPS-Modulen moderner Fahrzeuge durch das FBI erfolgt ohne richterlichen Beschluss.

> *...the pushpins on the new FBI geo-maps indicate where people live, work, pray, eat and shop, not necessarily where they commit or plan crimes* [37].

Im September 2012 hat in den USA der Sixth Circuit Court of Appeals entschieden, das bezügliche Standortdaten keine Ansprüche auf Privatsphäre bestehen. Diese Entscheidung ermöglicht es US-Firmen, diese Daten hemmungslos zu sammeln. Die Dienste der USA dürfen ohne richterliche Prüfung Standortdaten von GPS-Geräten verfolgen.

Die Daten werden mit verschiedenen Methoden gesammelt:

[36] https://www.heise.de/tr/artikel/Immer-im-Visier-276659.html
[37] http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims

- Hauptlieferanten für Geodaten sind Smartphones und Handys. Vor allem Apps können genutzt werden, um Geodaten zu sammeln. Über die Hälfte der in verschiedenen Stores downloadbaren Apps versenden Standortdaten unabhängig davon, ob sie für die Funktion der App nötig sind. Der Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet.

- Mit Einführung des iPhone 4 hat Apple seine Datenschutzbestimmungen geändert. Die gesamte Produktpalette von Apple (iPhone, Laptops, PC...) wird in Zukunft den Standort des Nutzers laufend an Apple senden. Apple wird diese Daten Dritten zur Verfügung stellen. Wer Zugang zu diesen Daten hat, wird nicht näher spezifiziert.[38]

  Für die Datensammlungen rund um das iPhone wurde Apple mit dem BigBrother Award 2011 geehrt. Auszug aus der Laudation von F. Rosengart und A. Bogk:

  > *Apples Firmenstrategie scheint darauf ausgelegt zu sein, möglichst viele Daten der Nutzer zu erfassen, ähnlich wie es soziale Netzwerke auch tun. Werbepartner freuen sich darauf, mit Hilfe von Apple möglichst zielgruppengerechte und standortbezogene Werbung auf dem Telefon anzeigen zu können.*

  Das chinesische Staatsfernsehen bezeichnete die Möglichkeit des Auslesens häufig besuchter Orte im iPhone als Risiko für die nationale Sicherheit [39], da die Daten bei US-Firmen gespeichert werden, die im Rahmen von PRISM mit der NSA kooperieren.

- Millionen von Fotos werden über verschiedene Dienste im Internet veröffentlicht (Flickr, Twitter, Facebook...). Häufig enthalten diese Fotos in den EXIF-Attributen die GPS-Koordinaten der Aufnahme. Die Auswertung dieses Datenstromes steht erst am Anfang der Entwicklung. Ein Beispiel ist die mit Risikokapital ausgestattete Firma Heypic, die Fotos von Twitter durchsucht und auf einer Karte darstellt.

- Die ganz normale HTTP-Kommunikation liefert Standortinformationen anhand der IP-Adresse. Aktuelle Browser bieten zusätzlich eine Geolocation-API, die genauere Informationen zur Verfügung stellt. Als Facebook im Sommer 2010 die Funktion Places standardmäßig aktivierte, waren viele Nutzer überrascht, wie genau jede reale Bewegung im Sozialen Netz lokalisiert wird. Nicht nur Facebook kann das.

  Die Deaktivierung von Places scheint bei Facebook wirklich umständlich zu sein. Damit wird aber nicht die Erfassung der Daten deaktiviert, sondern nur die Sichtbarkeit für andere Nutzer!

[38] http://www.apple.com/chde/legal/privacy/
[39] https://heise.de/-2257924

Abbildung 2.6: Lokalisierung eines Smartphones durch Facebook

- Lokalisierungsdienste wie *Gowalla* oder *Foursquare* bieten öffentlich einsehbare Standortdaten und versuchen, durch spielartigen Charakter neue Nutzer zu gewinnen. Im Gegensatz zu den oben genannten Datensammlungen kann man bei Gowalla oder Foursquare aber gut kontrollieren, welche Daten man veröffentlicht oder die Dienste nicht nutzen.

Nichts zu verbergen?

Wer ein praktisches Beispiel braucht: Einer Kanadierin wurde das Krankengeld gestrichen, weil sie auf Facebook fröhliche Urlausbfotos veröffentlichte. Die junge Frau war wegen Depressionen krank geschrieben und folgte dem Rat ihres Arztes, einmal Urlaub zu machen und Zusammenkünfte mit Freunden zu suchen. Die Krankenkasse nutzte keine technischen Geo-Informationen sondern stellte visuell durch Beobachtung des Facebook-Profils den Aufenthaltsort fest. Aber das Beispiel zeigt, dass die automatisierte Auswertung Konsequenzen haben könnte.[40]

Einen ähnlichen Fall gab es 2012 in Östereich. Aufgrund der bei Facebook veröffentlichten Fotos von einem Diskobesuch wurde gegen eine Linzer Kellnerin Klage wegen Krankenstandsmissbrauch erhoben.[41]

2.7 Kommunikationsanalyse

Geheimdienste verwenden seit Jahren die Kommunikations-Analyse (wer mit wem kommuniziert), um die Struktur von Organisationen aufzudecken.

> *Auch ohne Kenntnis der Gesprächs- oder Nachrichteninhalte - die nur durch Hineinhören zu erlangen wäre - lässt sich allein aus dem zeitlichen Kontext und der Reihenfolge des Kommunikationsflusses eine hohe Informationsgüte extrahieren, nahezu vollautomatisch.* (Frank Rieger)

Die Verwendung der Daten demonstriert das **Projekt Gegenwirken** der niederländischen Geheimdienste. In regierungskritischen Organisationen

[40] http://www.magnus.de/news/krankengeld-gestrichen-wegen-verfaenglichen-facebook-bildern-208271.html
[41] http://www.unwatched.org/20120601_Unachtsamer_Umgang_mit_Facebook_kann_unangenehme_Folgen_haben

werden die Aktivisten identifiziert, deren Engagement für die Gruppe wesentlich ist. Für die Kommunikationsanalyse nötige Daten werden dabei u.a. mit systematisch illegalen Zugriffen gewonnen. Die identifizierten Aktivisten werden mit kleinen Schikanen beschäftigt, um die Arbeit der Gruppe zu schwächen. Das Spektrum reicht von ständigen Steuerprüfungen bis zu Hausdurchsuchungen bei harmlosen Bagatelldelikten.

Im Rahmen der Vorratsdatenspeicherung (VDS) werden genau die Datenbestände angelegt, die den Geheimdiensten und dem BKA eine umfassende Kommunikationsanlayse ermöglichen. Zur Kriminalitätsbekämpfung und -prävention taugt die Vorratsdatenspeicherung nicht, wie ein Vergleich der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008, 2009 und 2010 zeigt.

Zivile Kommunikations-Analyse

Zunehmend wird auch im zivilen Bereich diese Analyse eingesetzt. Das Ziel ist es, Meinungsmacher und kreative Köpfe in Gruppen zu identifizieren, gezielt mit Werbung anzusprechen und sie zu manipulieren. Im Gegensatz zu den Diensten haben Unternehmen meist keinen Zugriff auf Verbindungsdaten von Telefon und Mail. Es werden öffentlich zugängliche Daten gesammelt. Facebook und Twitter bietet ein umfangreichen Datenpool oder die Kommentare in Blogs und Foren. Teilweise werden von Unternehmen gezielt Blogs und Foren zu bestimmten Themen aufgesetzt, um Daten zu generieren.

Wie man die Freundschaftsbeziehungen in sozialen Netzen wie Facebook oder ...VZ werden analysieren kann, um omosexuelle Orientierung zu erkennen, haben ehemalige Studenten des MIT mit *Gaydar - die Schwulenfalle* demonstriert. Die TU Berlin hat zusammen mit der Wirtschaftsuniversität Wien erfolgversprechende Ergebnisse zur *Rasterfahndung nach Meinungsmachern* veröffentlicht.

Ein Beispiel

Kommunikationsanalyse ist ein abstrakter Begriff. Anhand eines stark vereinfachten Beispiels soll eine Einführung erfolgen, ohne den Stand der Forschung zu präsentieren. Das Beispiel zeigt die Analyse einer subversiven Gruppe auf Basis einer Auswertung der Kommunikationsdaten von wenigen Mitgliedern. Die Kommunikationsdaten können aus verschiedenen Kanälen gewonnen werden: Telefon, E-Mail, Briefe, Instant-Messaging, Soziale Netze…

Als Beispiel nehmen wir eine Gruppe mit dem Namen *"Muppet Group"*, abgekürzt *"mg"*. Als Ausgangslage ist bekannt, dass *Anton* und *Beatrice* zur *"mg"* gehören.

Durch Auswertung aller zur Verfügung stehenden Kommunikationsdaten von *Anton* und *Beatrice* erhält man ein umfangreiches Netz ihrer sozialen Kontakte (Bild 2.7). Dabei wird nicht nur die Anzahl der Kommunikationsprozesse ausgewertet, es wird auch die zeitliche Korrelation einbezogen.

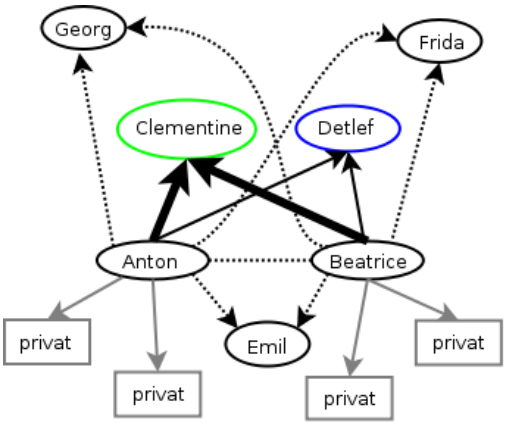


Abbildung 2.7: Soziales Netz von Anton und Beatrice

Besonders häufig haben beide (zeitlich korreliert) Kontakt zu *Clementine* und *Detlef*. Diese beiden Personen scheinen eine wesentliche Rolle innerhalb der Gruppe "mg" zu spielen. Einige Personen können als offensichtlich privat aus der weiteren Analyse entfernt werden, da nur einer von beiden Kontakt hält und keine zeitlichen Korrelationen erkennbar sind.

Ideal wäre es, an dieser Stelle die Kommunikation von *Clementine* und *Detlef* näher zu untersuchen. Beide sind aber vorsichtig und es besteht kein umfassender Zugriff auf die Kommunikationsdaten. Dann nimmt man als Ersatz vielleicht *Frida*, um das Modell zu präzisieren.

Frida unterhält vor allem einen engen Kontakt zu *Detlef*, was zu einer Umbewertung der Positionen von *Detlef* und *Clementine* führt (Bild 2.8). Bei *Emil* handelt es sich evtl. um einen zufällig gemeinsamen Bekannten von *Anton* und *Beatrice*, der nicht in die "mg" eingebunden ist.

Reale Datenmmengen

Reale Kommunikationsnetzwerke sind wesentlich komplexer. Auf Grundlage der Daten, die von T-Mobile über den Politiker Malte Spitz gespeichert wurden, hat Michael Kreil von OpenDataCity die Grafik in Bild 2.9 mit den Rohdaten erstellt.

Etwas besser aufbereitete Daten visualisiert Bild 2.10 mit den Kommunikationsdaten einer Woche von Ton Siedsmas.

Wenn man auch die Standortdaten des Smartphone mit auswerten kann, werden die Informationen deutlich detaillierter. Bild 2.11 zeigt einen Tag von Ton Siedsmas.

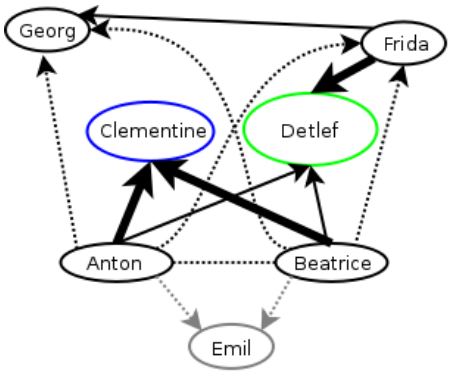


Abbildung 2.8: Präzisierte Struktur der "mg"

Analysetools wie *i2 Analyst's Notebook* von IBM oder *rola rsCASE* können diese Daten sehr schön aufbereiten und die Schlapphüte bei der Analyse effektiv unterstützen (Bild 2.12).

2.8 Überwachungen im Internet

Unter http://www.daten-speicherung.de/index.php/ueberwachungsgesetze findet man eine umfassende Übersicht zu verschiedenen Sicherheitsgesetzen der letzten Jahre. Neben einer Auflistung der Gesetze wird auch dargestellt, welche Parteien des Bundestages dafür und welche Parteien dagegen gestimmt haben. Sehr schön erkennbar ist das Muster der Zustimmung durch die jeweiligen Regierungsparteien und meist Ablehnung durch die Opposition, von Böswilligen als Demokratie-Simulation bezeichnet. Unabhängig vom Wahlergebnis wird durch die jeweiligen Regierungsparteien die Überwachung ausgebaut, denn **Du bist Terrorist!** [42]

Vorratsdatenspeicherung: (Neusprech: *Daten-Mindestspeicherfrist* oder ganz neu: *private Vorsorgespeicherung*)

Ohne jeglichen Verdacht sollen die Verbindungsdaten jeder E-Mail, jedes Telefonats, jeder SMS und Standortdaten der Handys gesammelt werden. Die Versuche zur Einführung sind nicht neu, seit mehr als 18 Jahren versuchen unterschiedliche Regierungen diese Überwachungsmaßnahme einzuführen, ohne die Notwendigkeit für die Strafverfolgung begründen zu können. Nutznießer sind in erster Linie die Geheimdienste.

- 1997 wurde die Vorratsdatenspeicherung aufgrund verfassungsrechtlicher Bedenken abgelehnt.
- 2002 wurde ein ähnlicher Gesetzentwurf vom Deutschen Bundestag abgelehnt und die Bundesregierung beauftragt, gegen

[42] http://www.dubistterrorist.de

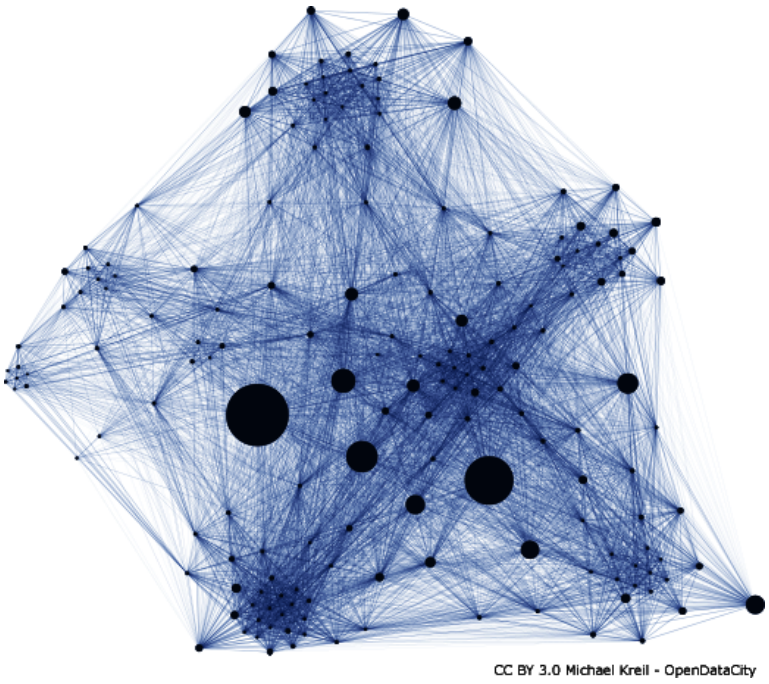


Abbildung 2.9: Kommunikationsnetzwerk von Malte Spitz

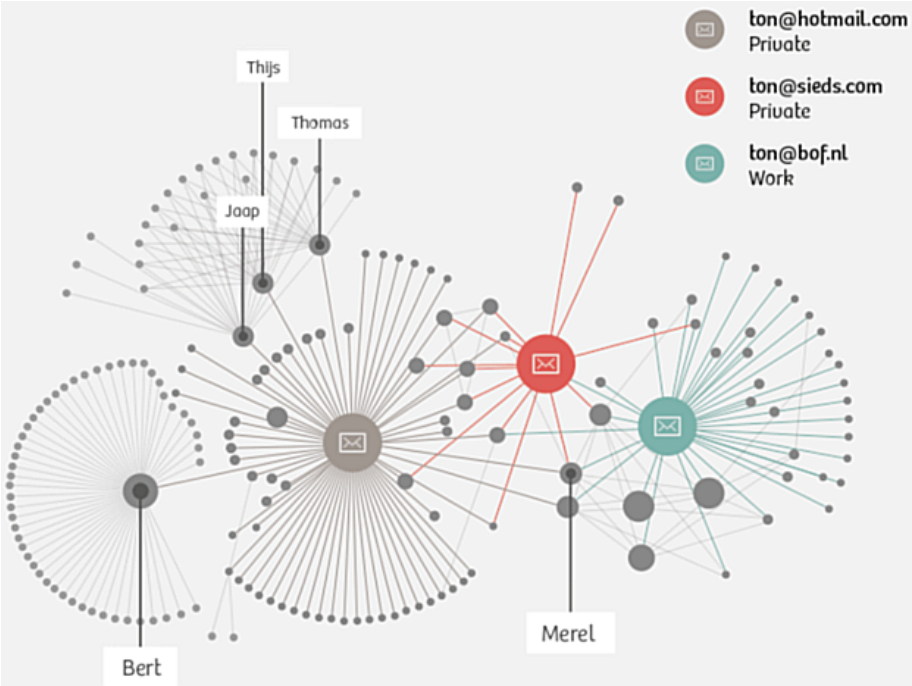


Abbildung 2.10: Aufbereitete Kommunikationsdaten von Ton Siedsmas

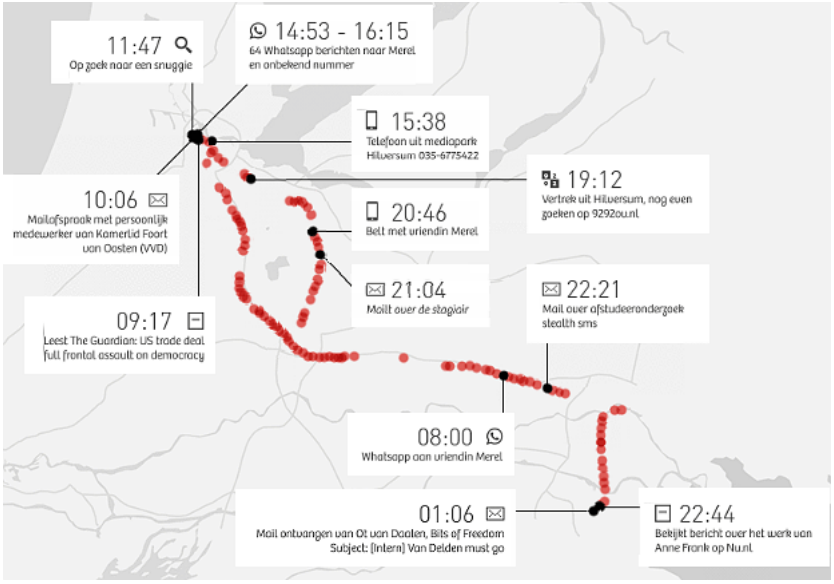


Abbildung 2.11: Standortdaten eines Tages von T. Siedsmas

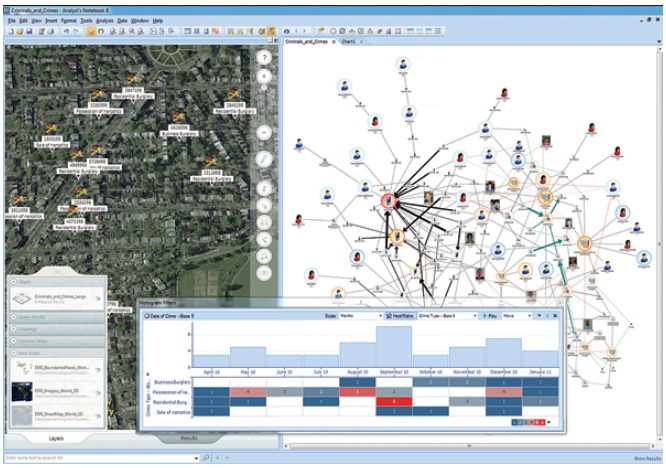


Abbildung 2.12: Screenshot von *i2 Analyst's Notebook* (IBM)

einen entsprechenden Rahmenbeschluß auf EU-Ebene zu stimmen (Bundestag-Drucksache 14/9801).

- 2005 hat das EU-Parlament mit Mehrheit der christ- und sozialdemokratischen Fraktionen die Richtlinie zur 6-monatigen Datenspeicherung der Verbindungs- und Standortdaten (VDS) beschlossen (Directive 2006/24/EG). Um die Richtlinie mit einfacher Mehrheit in der EU-Kommision ohne Mitsprache des Parlamentes verabschieden zu können, wurde sie nicht als Sicherheits- und Polizeimaßnahme behandelt sondern als Maßnahme zur *Regulierung des Binnenmarktes* definiert, was außerdem die EU-Länder zu einer Umsetzung zwingt.
- 2006 hat der Wissenschaftliche Dienst des Bundestages ein Rechtsgutachten mit schweren Bedenken gegen die VDS vorgelegt.
- Ein Vergleich der Zahlen der Kriminalitätsstatistik des BKA für die Jahre 2007, 2008 und 2009 zeigt, dass die VDS im Jahr 2009 nicht zur einer Verbesserung der Aufklärungsrate von Straftaten im Internet führte und keine Einfluss auf die Tendenz der Entwicklung hatte. Es gibt mehr Straftaten im Internet bei abnehmender Aufklärungsrate.

	2008 (o. VDS)	2009 (**mit VDS**)	2010 (o. VDS)
Straftaten im Internet	167.451	206.909	223.642
Aufklärungsrate (Internet)	79.8%	75.7%	72,3%

- 2010 erklärt das Bundesverfassungsgericht in einem Grundsatzurteil das Gesetz zur VDS als nicht vereinbar mit dem Grundgesetz. (Az: 1 BvR 256/08)[43]
- 2012 zeigte das Max-Planck-Instituts (MPI) für ausländisches und internationales Strafrecht in einer umfangreichen wissenschaftlichen Analyse, dass KEINE *Schutzlücke* ohne Vorratsdatenspeicherung besteht und widerspricht damit der Darstellung von mehreren Bundesinnenministern und BKA-Chef Ziercke, wonach die VDS für die Kriminalitätsbekämpfung unbedingt nötig wäre. Die in der Presse immer wieder herangezogenen Einzelbeispiele halten einer wissenschaftlichen Analyse nicht stand.[44]
- 2012 gibt es einen nicht erfolgreichen Anlauf, die VDS international im Rahmen der UNODC als verpflichtende Richtlinie zu etablieren. Der Verfassungsschutz hat diesen Versuch offensiv unterstützt.[45]
- 2014 wird die Richlinie 2006/24/EG vom EuGH als nicht vereinbar mit der Charta der Grundrechte der Europäischen Union gekippt. (Urteil C-293/12 und C-594/12)
- 2015 wird im Eilverfahren ein neues Gesetz zur *Speicherpflicht für Verkehrsdaten* verabschiedet. Bundesjustizminister H. Maas konnte auf der Pressekonferenz zur Verabschiedung des Gesetzentwurfes

[43] http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
[44] http://www.ccc.de/de/updates/2012/mythos-schutzluecke
[45] https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/

im Bundeskabinett auf Nachfrage keinen Grund nennen, warum die Vorratsdatenspeicherung notwendig sein soll:

> Frage: *Kann der Minister die Notwendigkeit der Vorratsdatenspeicherung beweisen (was eine Vorraussetzung für Grundrechtseingriffe wäre)?*
>
> Antwort H. Maas: *Die Notwendigkeit kann ich nicht beweisen.*

Für die Bundesdatenschutzbeauftragte A. Voßhoff ist die VDS verfassungswidrig und widerspricht Urteilen von BVerfG und EuGH. Der ehemalige Bundesdatenschutzbeauftragte P. Schaar kommentierte:

> *Brauchen wir das überhaupt? Die Bundesregierung bleibt den Nachweis schuldig, dass dieser erhebliche Grundrechtseingriff unerlässlich ist.*

- Am 16.10.2015 hat der Bundestag erneut das neue Gesetz zur Vorratsdatenspeicherung beschlossen. Verfassungsklagen wurden inzwischen eingereicht.
- 2017 legt der Wissenschaftliche Dienst zum wiederholten Mal ein Gutachten zur Vorratsdatenspeicherung vor, dass zu dem Schluss kommt, dass das aktuelle Gesetz nicht nicht mit geltendem EU-Recht vereinbar ist. In mehreren Punkten verstößt das neue Gesetz gegen die Vorgaben des Europäischen Gerichtshofes.[46]

Warum bemüht man sich seit Jahren, eine Überwachungsmaßnahme einzuführen, die uns einige hundert Millionen Euro kosten wird, die so gut wie keine Beitrag zur Verbesserung der Strafverfolgung bietet und in erster Linie den Geheimdiensten (Neusprech: *Gefahrenabwehrdiensten*) neue Kompetenzen verschaffen wird?

Bestandsdatenauskunft Der IT-Sicherheitsforscher Pete Swire hat im April 2012 ein Paper[47] veröffentlicht, in dem er die aktuellen Tendenzen in der Überwachung aufzeigt. Weil das *Lauschen am Draht* in allen Variationen zunehmend uneffektiv wird, wollen Geheimdienste und Strafverfolger Zugriff auf die *Daten in der Cloud*. Dazu zählen auch E-Mail Accounts. Die Hürden für den Zugriff sollen dabei möglichst gering sein.

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 kommt der Gesetzgeber den Wünschen der Geheimdienste weit entgegen. Die Cloud-Provider und Mail-Provider sollen automatisiert nutzbare Schnittstellen für die Abfrage von Bestandsdaten bereitstellen. Zu den Bestandsdaten zählen seit Dezember 2012 neben Name und Anschrift usw. auch folgende Daten, die im Gegensatz zu den allgm. Bestandsdaten aber nur mit Richtervorbehalt abgefragt werden sollen:

- Passworte für den Zugriff auf E-Mail Konten und Cloud-Speicher.

[46] https://netzpolitik.org/2017/gutachten-gesetz-zur-vorratsdatenspeicherung-erfuellt-vorgaben-des-eugh-nicht/

[47] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2038871

- PINs zum Entsperren von Smartphones.
- Zugriff auf die Endgeräte (Router), die den Kunden vom DLS-Provider kostenlos bereitgestellt werden (TR-069 Schnittstelle).

Die PiratenPartei kommentierte den Gesetzentwurf kurz und bündig:

Der Entwurf der Bundesregierung ist schlicht verfassungswidrig.

Zensur im Internet: Die Zensur sollte in Deutschland im Namen des Kampfes gegen Kinderpornografie im Internet eingeführt werden. Man wurde nicht müde zu behaupten, es gäbe einen Millionen Euro schweren Massenmarkt, der durch Sperren von Webseiten empfindlich ausgetrocknet werden kann. Die Aussagen wurden geprüft und für falsch befunden [48].

1. In der ersten Stufe unterzeichneten im Frühjahr 2009 die fünf großen Provider freiwillig einen geheimen Vertrag mit dem BKA. Sie verpflichteten sich, eine Liste von Webseiten zu sperren, die vom BKA ohne nennenswerte Kontrolle erstellt werden sollte.
2. In der zweiten Stufe wurde am 18.06.09 das *Zugangserschwernisgesetz* verabschiedet. Alle Provider mit mehr als 10.000 Kunden sollen diese geheime Liste von Websites zu sperren. Neben den (ungeeigneten) DNS-Sperren sollen auch IP-Sperren und Filterung der Inhalte zum Einsatz kommen.
3. Die CDU/FDP-Regierung ist im Herbst 2009 einen halben Schritt zurück gegangen und hat mit einem Anwendungserlass die Umsetzung des Gesetzes für ein Jahr aufgeschoben. Diese Regierung meint also, über dem Parlament zu stehen und ein beschlossenes Gesetz nicht umsetzen zu müssen.
4. Im Rahmen der Evaluierung des Gesetzes geht das BKA nur halbherzig gegen dokumentierten Missbrauch vor, wie eine Veröffentlichung des AK-Zensur zeigt. Gleichzeitig wird weiter Lobbyarbeit für das Zensurgesetz betrieben [49].
5. Die Auswertung des eco Verband zeigt, dass Webseiten mit dokumentiertem Missbrauch effektiv gelöscht werden können. 2010 wurden 99,4% der gemeldeten Webseiten gelöscht [50]. Auch 2011 und 2012 konnte das BKA 99% aller gemeldeten KiPo-Webseiten löschen lassen. Warum also die Internet–Stoppschilder?
6. Im Herbst 2011 wurde das Gesetz offiziell beerdigt.

Der Aufbau einer Infrastruktur für Zensur im Internet wird auf vielen Wegen betrieben. Neben dem Popanz *"Kinderpornografie"* engagiert sich die Content Maffia im Rahmen der geheimen ACTA Verhandlungen für eine verbindliche Verpflichtung zum Aufbau der Infrastruktur für Websperren. Die CDU/CSU Bundestagsfraktion sieht die amerikanischen Gesetzesvorlagen SOPA und PIPA als richtungsweisend an. Beide Gesetzesvorlagen sehen umfangreiche Zensurmaßnahmen zum Schutz

[48] http://blog.odem.org/2009/05/quellenanalyse.html
[49] http://ak-zensur.de/2010/08/kapitulation.html
[50] http://www.eco.de/verband/202_8727.htm

geistigen Eigentums vor.

Die verfassungsrechtlichen Bedenken gegen die Zensur hat der wissenschaftliche Dienst des Bundestages in einem Gutachten zusammengefasst[51]. Auch eine Abschätzung der EU-Kommision kommt zu dem Schluss, dass diese Sperrmaßnahmen **notwendigerweise eine Einschränkung der Menschenrechte voraussetzen**, beispielsweise der freien Meinungsäußerung.

BKA Gesetz: Mit dem BKA Gesetz wurde eine Polizei mit den Kompetenzen eines Geheimdienstes geschaffen. Zu diesen Kompetenzen gehören neben der heimlichen Online-Durchsuchung von Computern der Lauschangriff außerhalb und innerhalb der Wohnung (incl. Video), Raster- und Schleierfahndung, weitgehende Abhörbefugnisse, Einsatz von V-Leuten, verdeckten Ermittlern und informellen Mitarbeitern...

Im Rahmen präventiver Ermittlungen (d.h. ohne konkreten Tatverdacht) soll das BKA die Berechtigung erhalten, in eigener Regie zu handeln und Abhörmaßnahmen auch auf Geistliche, Abgeordnete, Journalisten und Strafverteidiger auszudehnen. Im Rahmen dieser Vorfeldermittlungen unterliegt das BKA nicht der Leitungsbefugnis der Staatsanwaltschaft.

Damit wird sich das BKA bis zu einem gewissen Grad jeglicher Kontrolle, der justiziellen und erst recht der parlamentarischen, entziehen können [52].

Telekommunikationsüberwachungsverordnung Auf richterliche Anordnung wird eine Kopie der gesamten Kommunikation an Strafverfolgungsbehörden weitergeleitet. Dieser Eingriff in das verfassungsmäßig garantierte Recht auf unbeobachtete Kommunikation ist nicht nur bei Verdacht schwerer Verbrechen möglich, sondern auch bei einigen mit Geldstrafe bewährten Vergehen und sogar bei Fahrlässigkeitsdelikten (siehe §100a StPO).

Laut Gesetz kann die Überwachung auch ohne richterliche Genehmigung begonnen werden. Sie ist jedoch spätestens nach 3 Tagen einzustellen, wenn bis dahin keine richterliche Genehmigung vorliegt.

Präventiv-polizeil. Telekommunikationsüberwachung ermöglicht es den Strafverfolgungsbehörden der Länder Bayern, Thüringen, Niedersachsen, Hessen und Rheinland-Pfalz den Telefon- und E-Mail-Verkehr von Menschen mitzuschneiden, die keiner(!) Straftat verdächtigt werden. Es reicht aus, in der Nähe eines Verdächtigten zu wohnen oder möglicherweise in Kontakt mit ihm zu stehen.

Die Anzahl der von dieser Maßnahme Betroffenen verdoppelt sich Jahr für Jahr. Gleichzeitig führen nur 17% der Überwachungen zu Ergebnissen im Rahmen der Ermittlungen.

[51] http://netzpolitik.org/wp-upload/bundestag_filter-gutachten.pdf
[52] http://www.berlinonline.de/berliner-zeitung/print/politik/725127.html

Datenbanken: Begleitet werden diese Polizei-Gesetze vom Aufbau umfangreicher staatlicher Datensammlungen. Von der Schwarze Liste der Ausländerfreunde (Einlader-Datei) bis zur AntiTerrorDatei, die bereits 20.000 Personen enthält, obwohl es in Deutschland keinen Terroranschlag gibt. (Abgesehen von den Muppets aus dem Sauerland, deren Islamische Jihad Union offensichtlich eine Erfindung der Geheimdienste ist.)

Elektronisicher PA: Mit dem Elektronischen Personalausweis wird die biometrische Voll-Erfassung der Bevölkerung voran getrieben. Außerdem werden die Grundlagen für eine eindeutige Identifizierung im Internet gelegt, begleitet von fragwürdigen Projekten wie De-Mail.

Der Elektronische Polizeistaat

> *Würde man noch den Mut haben, gegen die Regierung zu opponieren, wenn diese Einblick in jede Email, in jede besuchte Porno-Website, jeden Telefonanruf und jede Überweisung hat?*

Was unterscheidet einen elektronischen Polizeistaat von einer Diktatur? Gibt es dort auch eine Geheime Bundespolizei, die Leute nachts aus der Wohnung holt und abtransportiert, ohne juristischen Verfahren einsperrt...

Ein elektronischer Polizeistaat arbeitet sauberer. Es werden elektronische Technologien genutzt um forensische Beweise gegen BürgerInnen aufzuzeichnen, zu organisieren, zu suchen und zu verteilen. Die Informationen werden unbemerkt und umfassend gesammelt, um sie bei Bedarf für ein juristisches Verfahren als Beweise aufzubereiten.

Bei einem Vergleich von 52 Staaten hinsichtlich des Ausbaus des elektronischen Polizeistaat hat Deutschland einen beachtlichen 10 Platz belegt. Es verwundert nicht, dass an erster Stelle China und Nordkorea, gefolgt von Weißrussland und Russland stehen. Dann aber wird bereits Großbritannien aufgelistet, gefolgt von den USA, Singapur, Israel, Frankreich und Deutschland.

> *Noch sei der Polizeistaat nicht umfassen realisiert, "aber alle Fundamente sind gelegt". Es sei schon zu spät, dies zu verhindern. Mit dem Bericht wolle man die Menschen darauf aufmerksam machen, dass ihre Freiheit bedroht ist.*

Das dieser Polizeistaat bereits arbeitsfähig ist, zeigt die Affäre Jörg Tauss. Ein unbequemer Politiker mit viel zu engen Kontakten zum CCC, der Datenschutz ernst nimmt, gegen das BKA-Gesetz und gegen Zensur auftritt, wird wenige Monate vor der Wahl des Konsums von KiPo verdächtigt. Die Medien stürzen sich auf das Thema. Innerhalb kurzer Zeit war Tauss als Politiker von der Springer-Presse demontiert, unabhängig von der später folgenden Verurteilung.

Ähnliche Meldungen hatten in den letzten Jahren viel weniger Resonanz:

1. *Auf dem Dienstcomputer eines hochrangigen Mitglieds des hessischen Innenministeriums sind vermutlich Kinderpornos entdeckt worden.* (25.07.2007)

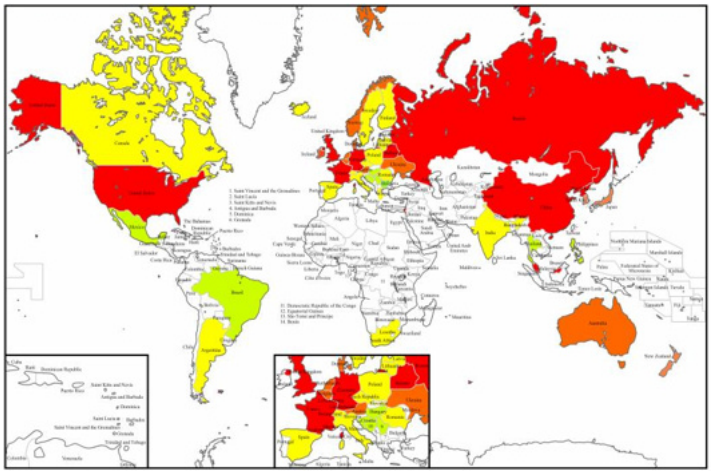


Abbildung 2.13: Vergleich der elektronischen Polizeistaaten

2. *Kinderpornos: CDU-Politiker unter Verdacht* (01.04.2005)
3. *Der CDU-Politiker Andreas Zwickl aus Neckarsulm ist wegen Verdachts des Besitzes von Kinderpronografie...* (05.03.2009)

2.9 Terrorismus und Ausbau der Überwachung

Nach den Anschlägen von Paris im Nov. 2015 eskaliert der Ausbau der Überwachung und wird als die angebeblich einzige Alternative zum Schutz der Bevölkerung diskutiert. Die EU erlaubt Frankreich sogar die Verletzung der Euro-Stabilitätskriteriern[53], weil durch den notwendigen(?) Ausbau des Überwachungsstaates nach den Anschlägen außergewöhnliche finanzielle Belastungen entstehen. Die Medien schockieren uns mit einem einzelnen Ereignis. Wenn man Zeit und etwas Ruhe zum Nachdenken findet, dann relativiert sich der Schock.

Jemand hat die Toten durch Terroranschläge in Europa in den letzten Jahrzehnten aufgeschlüsselt. Die Grafik 2.14 auf Basis der Daten der *Global Terrorism Database*[54] zeigt, dass Europa hinsichtlich Terrorgefahr noch nie so sicher war, wie heute.

Die jährlichen *EU Terrorism Reports* von Europol zeigen das gleiche Bild. 2005/2006 gab es fast 500 Terroranschläge pro Jahr in Europa, also mehr als ein Anschlag pro Tag und mehr als 700 Verhaftungen (siehe: TE-SAT Report für 2006 [55]). Hauptverantwortlich waren die ETA, die IRA und die italienischen Korsen. In dieser Zeit wurde ein Anschlag mit 191 Toten in Madrid zwar zur

[53] http://www.faz.net/aktuell/wirtschaft/haushaltspolitik-schutz-der-buerger-wichtiger-als-defizitziele-13917723.html
[54] http://www.start.umd.edu/gtd
[55] https://www.europol.europa.eu/sites/default/files/publications/tesat2007.pdf

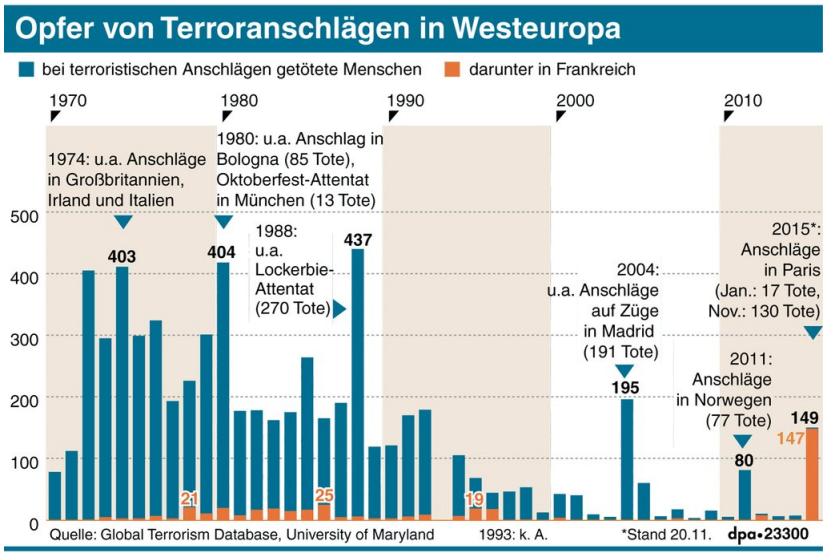


Abbildung 2.14: Opfer von Terroranschlägen in Westeuropa

Kenntnis genommen, ein bisschen diskutiert und am nächsten Tag wieder vergessen.

Bis 2010 konnte durch politische Maßnahmen die Zahl der Terroranschläge im Vergleich zu 2006 halbiert werden, es gab nur noch 246 Anschläge[56]. Der Europol-Bericht TE-SAT 2014 listet nur noch 152 Terroranschläge mit 7 Toten auf, das ist der bis niedrigste Stand.[57]

2015 wurde wieder ein Anstieg bei Terroranschlägen verzeichnet (insgesamt 211 Anschläge). Während sich linke und separatitische Anschläge weiter verringerten (nur noch 65), kam es zu einer Zunahme von jihadistischen Anschlägen vor allem in Frankreich. Dabei starben 148 Personen, da jihadiststische Selbstmordattentäter eine möglichst hohe Zahl von Todesopfern erzielen wollen. 687 potentielle islamistische Attentäter wurden verhaftet, davon wurden 98% verurteilt.[58]

Die Terrorgefahr in Europa wurde im letzten Jahrzehnt nicht durch den Ausbau der Überwachung reduziert, sondern durch einen politischen Integrationsprozess der separatistischen Gruppen. Warum wird dieses erfolgreiche Konzept jetzt nicht mehr diskutiert? Das Frankreich und Belgien auf diesem Gebiet der Integration massive Defizite haben, ist seit Jahren bekannt. Der vom franz. Präsidenten Hollande ausgerufenen *Krieg gegen den Islamismus* ist keine Lösung, auch nicht mit 5.000 Mann mehr Personal für die Dienste.

[56] https://www.counterextremism.org/resources/details/id/229
[57] https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014
[58] https://www.europol.europa.eu/content/te-sat-2014-european-union-terrorism-situation-and-trend-report-2014

Eine wesentliche Rolle bei der Wahrnehmung von Terror spielen die Medien. Neben den redaktionell betreuten Medien wie Mainstream Presse und den qualitativ guten Blogs (bzw. alternativen Medien) haben sich Twitter und Facebook als sogenannte **Panik-Medien** etabliert. Schockierende Ereignisse verbreiten sich über diese Medien viral und schnell. Die etablierten, journalistischen Medien geraten unter Druck und müssen darauf reagieren. Neben der *Terror* gab es in der Vergangenheit weitere Beispiele von Panikattacken wie *Schweinegrippe* oder *Ebola*. Das 700.000 Kinder in der Sahel-Zone verhungern, interessiert kaum.

Manchmal bin ich schockiert, wie stark die emotionale Wirkung der Panik-Medien geworden ist. Eine Mutter sprach einigen Tagen nach dem Anschlag in Paris in privater Runde über die Angst, dass ihre 17-jährige Tochter einem Terroranschlag zum Opfer fallen könnte, wenn sie abends allein in Berlin unterwegs ist. Ähmm - .... also ich würde eher auf Autounfall oder Unfall mit dem Fahrrad tippen, diese Gefahr ist unverändert hoch. Das Fahrrad vom Töchterchen hat nämlich kein funktionierendes Rücklicht.

Die neuen Terroristen haben gelernt, die Panik-Medien für ihre Interessen immer besser zu nutzen. Auch die Apologethen der Überwachung nutzen die resultierende Angst für ihre eigenen Interessen und nicht für die Bekämfung des Terrorismus. Der Schock durch die Anschläge wurde von der deutschen Regierung genutzt, um den bereits geplanten Ausbau der Geheimdienste um 475 Mitarbeiter anzukündigen. Noch nie war die Manipulation der Emotionen so stark und großflächig wie heute. *Der moderne Krieg ist kein Krieg um Territorien sondern ein Krieg um die Köpfe.* Dieser Satz stammt aus der aktuellen Überarbeitung der NATO Doktrin, er trifft aber auch beim Kampf gegen Terror zu.

Militärische Aktionen und geheimdienstliche Eskalation in den Überwachungsstaat sind keine Lösungen. Menschlichkeit und Integration sind wirkungsvolle Mittel, um Terror zu bekämpfen. In der gobalen Politik müsste man jene konsequent ächten, die Terrorismus als Mittel zur Durchsetzung eigener Interessen fördern und anwenden. Die Grafik 2.15 zeigt die Länder, die seit 2010 Geld zur Finanzierung von Terrorismus bereitgestellt haben.

Ein konsequenter, politischer Druck auf Saudi Arabien (der größte Finanzier des ISIS), die USA und die Türkei könnte im Kampf gegen Terrorismus mehr erreichen, als alle Bomben zusammen. Das wird aber nicht diskutiert. Statt dessen werden Saktionen gegen Russland und den Iran aufrecht erhalten.

Auch Frankreich ist seit Jahrzehnten als Förderer von staatlich Terrorismus bekannt und hat in afrikanischen Ländern mehrere blutige Putsche organisiert, weil die gewählten Regierungen nicht den wirtschaflichen Interessen von Frankreich entsprachen.[59]

[59] https://www.heise.de/tp/artikel/46/46592/1.html

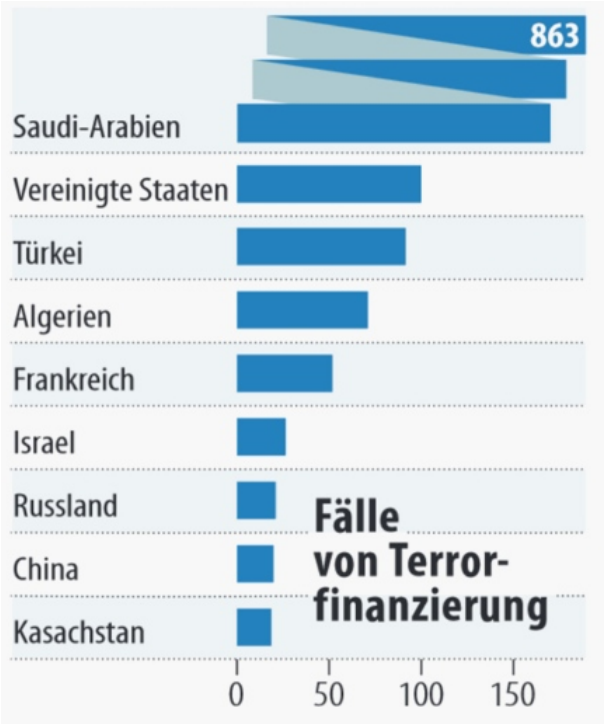


Abbildung 2.15: Staaten, die Terroristen finanzieren

2.10 NSA & Co.

In den 1970er Jahren wurde durch einen Whistleblower ein gigantischer Überwachungsskandal von NSA, CIA und FBI aufgedeckt. Die Medien berichteten, dass die NSA über Jahre routinemäßig den kompletten Nachrichtenverkehr von und nach den USA überwachten. Die NSA verfügte bereits damals über *außerordentliche Fähigkeiten zur Telekommunikationsüberwachung*. Die wichtigsten amerikanischen Fernmeldegesellschaften lieferten auf Basis eines Abkommens mit der NSA illegaler Weise täglich Kopien aller in den USA abgesandten oder empfangenen Telegramme an den Geheimdienst.

Der parlamentarische Untersuchungsausschuss zur Aufklärung dieser Überwachungspraktiken kam 1976 zu dem Ergebnis:

> *Die Regierung hat vielfach Bürger nur wegen ihrer politischen Überzeugung heimlich überwacht, auch wenn auf Grund dieser Überzeugungen weder Gewalt noch illegale Handlungen zu befürchten waren. [...] Ermittlungsen gegen Gruppen, die als potenziell gefährlich eingestuft wurden und Gruppen, die mit potenziell gefährlichen Organisationen zusammengearbeitet hatten, wurden über Jahrzehnte fortgesetzt, obwohl diese nicht in rechtswidrige Aktivitäten verwickelt waren.*

Auch damals versuchten Verantwortliche, eine Begrenzung der Überwachung mit allen Mitteln zu verhindern. Eine Einschränkung der Überwachung ge-

fährde die vitalen Interessen der USA. Trotzdem verabschiedete der Kongress 1978 den Foreign Intelligence Surveillance Act (FISA), um die ausufernde Überwachung etwas zu begrenzen. Ein Geheimgericht sollte für die Genehmigung von Überwachungsmaßnahmen gegen Amerikaner zuständig sein. Eine Begrenzung der Überwachung gegenüber Ausländern war ausdrücklich nicht vorgesehen.

Die FISA-Regeln wurden in der Folgezeit immer weiter aufgeweicht, insbesondere nach 9/11 durch den Patriot Act (2001) und den FISA-Amendmends Act (2008). Gemäß den aktuellen Auslegungen darf die NSA von den Telekommunikationsanbietern und Internetfirmen die Übermittlung kompletter Datenbanken verlangen, um darin selbst nach Einzelfällen zu suchen.

2013 ein Déjà-vu

Der von Snowden/Greenwald aufgedeckte Überwachungsskandal und die Beteiligung deutscher Geheimdienste als *second level partner* macht mich sprachlos. Man könnte viele Seiten füllen mit kurzen technischen Zusammenfassungen zu PRISM, QUANTUM, TAO, XKeyScore, ANT, BULLRUN, STORMBREW usw. Das würde nur zu folgender Schlussfolgerung führen:

Diese Geheimdienste agieren außerhalb jeder Kontrolle.

Besonders befremdlich ist für mich die Reaktion der deutschen Regierung. Als Konsequenz aus den Veröffentlichungen werden für den eigenen Gebrauch abhörsichere Crypto-Handys im Wert von 24 Mio. Euro bestellt. Der Bevölkerung gegenüber wird der NSA-Skandal ohne sichtbare Konsequenzen für beendet erklärt und ein Innenminister verkündet, dass sich jeder gefälligst selbst um die Sicherheit seiner Daten und privaten Kommunikation kümmern soll.

2.11 Rechtsstaatliche Grundlagen

Es ist erkennbar, wohin die Reise gehen soll. Die Räder rollen bereits.
Es wird Zeit, ein neues Ziel zu buchen, bevor der Zug abgefahren ist.

Die Kriminaliserung der Protestler gegen den G8-Gipfel in Heiligendamm als Terroristen, die Diskussion um die weiträumige Funkzellenauswertung anläßlich der Anti-Nazi-Demo in Dresden 2011, das Gutachten des Bundesdatenschutzbeauftragten zum *Staatstrojaner* und die Beteiligung deutscher Geheimdienste an den weltweiten Überwachungsprogrammen der NSA/GCHQ zeigen deutlich die gesellschaftlichen Defizite bei der Begrenzung der Überwachung.

Der teilweise erfolgreiche Widerstand der Zivilgesellschaft gegen Vorratsdatenspeicherung, Zugangserschwernisgesetz, Online Durchsuchung, Großer Lauschangriff usw. reicht nicht aus. Die gesellschaftlich ausgehandelten Normen (Gesetze, Urteile des BVerfG...) zur Begrenzung der Überwachung werden nicht respektiert und anscheinend systematisch und ohne Konsequenzen für die Verantwortlichen missachtet.

Gedanken für eine Gegenstrategie

1. Die Einhaltung der Normen für Polizei und Geheimdienste, die in einer demokratischen Diskussion ausgehandelt und als Gesetze bzw. Urteile des BVerfG niedergeschrieben sind, muss besser kontrolliert werden. Eine optionale Kontrolle ist unbrauchbar.

   Auf der Veranstaltung *Soziale Bewegungen im Digitalen Tsunami* hat Dr. Thilo Weichert (ULD) die Situation aus Sicht des Datenschutz treffend beschrieben:

   > *Die Polizeibehörden fragen uns nur, wenn sie wissen, dass wir unser o.k. geben.*

2. Verstöße der Strafverfolger gegen geltendes Recht (wie die Bundesdatenschutzbeauftragte bei der Kontrolle des BND in Bad Aibling aufdeckte) müssen geahndet werden, so wie es bei Verstößen gegen Gesetze auf anderen Gebieten üblich ist. Bisher agieren Strafverfolger anscheinend in einem "rechtsfreien Raum". Übertretungen der zulässigen Grenzen haben keine oder (bei starkem öffentlichen Druck) nur harmlose Konsequenzen.

   Der ehemalige Geheimdinestkontrolleur Wolfgang N. fordert ein Sonderstrafrecht für Geheimdienstmitarbeiter. Er fordert, dass Geheimmdienstmitarbeiter sich strafbar machen, wenn sie parlamentarische Kontrollgremien belügen und eine Kontrolle der Dienste behindern. Anderenfalls wird es so weitergehen wie bisher, dass BND und Verfassungschutz das Gesetz brechen können ohne Konsequenzen zu fürchten.

3. Strafrechtliche Konsequenzen für die durch Snowden aufgedeckte geheimdienstliche Bespitzelung auf internationaler und europäischer Ebene, Strafverfolgung aller Mitwisser, Täter und Profiteure in Justiz und Exekutive und aller Amtsträger in Deutschland, deren Aufgabe es gewesen wäre, uns vor ausländischer Spionage zu schützen.

4. Die Besetzung der Posten von Entscheidungsträgern bei Polizei und Geheimdiensten sollte mit Personen erfolgen, die sich dem ausgehandelten Konsens verpflichtet fühlen. Wenn der neue Polizeipräsident von Dresden die weiträumige Funkzellenüberwachung in Dresden für richtig hält und in einer ähnlichen Situation wieder zu diesem Mittel greifen will, obwohl es für rechtswidrig erklärt wurde, dann ist er für die Aufgabe ungeeignet.

   Udo Vetter stellt im lawblog die Frage:

   > *Wurde hier bewusst auf dem Rechtsstaat rumgetrampelt - oder sind die Verantwortlichen einfach so doof?*

5. Auf Basis des §129a StGB (Bildung einer terroristischen Vereinigung) wurden in den letzten Jahren so gut wie keine Verurteilungen ausgesprochen. Die sehr weit gehenden Befugnisse für Ermittlungen nach diesem

Paragraphen wurden jedoch mehrfach genutzt, um politische Aktivisten auszuforschen. Mehrfach haben verschiedene Gerichte die Anwendung des §129a StGB durch Ermittlungsbehörden für illegal erklärt.

- Doppeleinstellung in Sachen §129 [60]
- Razzien im Vorfeld des G8-Gipfels waren rechtswidrig [61]
- Konstruieren und Schnüffeln mit §129a [62]
- Durchsuchungen beim LabourNet waren rechtswidrig [63]

Dieser Missbrauch der Anti-Terror Befugnisse sollte gestoppt und evaluiert werden.

2.12 Bundesamt für Verfassungsschutz auflösen

Es wird Zeit, das Bundesamt für Verfassungsschutz aufzulösen. Seine Aufgabe als Bollwerk gegen die drohende Infiltration feindlicher Agenten aus der Sowjetunion oder der DDR besteht nicht mehr. Anti-Spionage und Anti-Terror Einsätze sowie Bekämpfung der Korruption und Verfolgung von Sachbeschädigungen sind Aufgabe von Polizei/BKA.

Die Humanistische Union fordert seit Jahren die Auflösung des BfV [64]. Die PiratenPartei Thüringen forderte im Beschluss des Parteitages im Nov. 2011 eine Auflösung des Thüringer Verfassungsschutzes[65] (wenige Tage bevor der NSU-Skandal bekannt wurde) und kritisiert die Übernahme der Strukturen in das Innenministerium. Die Linke in Hessen plädiert für die Auflösung des Verfassungsschutzes[66] und möchte statt dessen eine Informations- und Dokumentationsstelle einrichten für Bestrebungen gegen die Verfassung (ohne V-Leute und ohne geheimdienstliche Kompetenzen). Als Konsequenz aus dem NSA-Skandal forderte der Chaos Computer Club die Auflösung des BfV zur Wiedereinführung von Grundrechten und Rechtsstaatlichkeit[67].

Auflösungserscheinungen sind beim Verfassungschutz aber nicht erkennbar. Wie in jedem Jahr wird auch 2017 das Budget des Inlangeheimdienstes erhöht, diesmal um 45 Mio. Euro. Damit hat sich der Etat des Geheimdienstes im Vergleich zu 2000 verdreifacht!

V-Leute sind keine Lösung, sondern das Problem

- V-Leute des Verfassungsschutzes hatten erheblichen Anteil an der Radikalisierung der Studentenbewegung 1968. Vor allem der V-Mann Pe-

[60] http://de.indymedia.org/2008/10/228421.shtml
[61] http://www.ag-friedensforschung.de/themen/Globalisierung/g8-2007/bgh.html
[62] http://www.neues-deutschland.de/artikel/175230.konstruieren-und-schnueffeln-mit-s-129a.html
[63] http://www.labournet.de/ueberuns/beschlagnahme/index.html
[64] http://www.humanistische-union.de/fileadmin/hu_upload/doku/publik/huschrift17.pdf
[65] http://www.piraten-thueringen.de/2012/10/verfassungsschutz-auflosen-statt-umbetten/
[66] http://www.fr-online.de/rhein-main/hessen-linke-will-verfassungsschutz-aufloesen,1472796,17278430.html
[67] https://www.ccc.de/de/updates/2013/demonstration-wiedereinfuehrung–rechtsstaatlichkeit

ter Urbach wird immer wieder als Agent Provocateur genannt, der auch Waffen und Molotow-Cocktails lieferte und nach seiner Enttarnung vom Verfassungsschutz ins Ausland gebracht wurde.[68]

- Die Verflechtungen von Verfassungsschutz und *RAF* sind noch immer nicht aufgeklärt. Aus alten Unterlagen der Stasi geht hervor, dass Verena Becker vom Verfassungsschutz "kontrolliert wurde". V. Becker spielte eine wesentliche Rolle beim Mord an Generalbundesanwalt Buback.[69]

- Der Verfassungsschutz hat die rechtsradikale Szene nicht unterwandert, sondern finanziell unterstützt und vor Strafverfolgung geschützt.

  - Laut einem BKA-Report [70] von 1997 soll der Verfassungsschutz rechtsradikale Neonazis systematisch geschützt haben. Die Vorwürfe werden mit konkreten Fällen untermauert. V-Leute wurden vor Durchsuchungen gewarnt und einer Straftat überführte Nazis wurden nicht angeklagt und verurteilt, wenn sie als V-Leute arbeiteten. Informationen wurden zu spät an die Polizei weitergeleitet, so dass rechtsradikale Aktionen nicht mehr verhindert werden konnten.

  - Bereits 2002 hat das LKA Sachsen-Anhalt dem Verfassungsschutz misstraut und aus *ermittlungstaktischen Gründen* nicht über Exekutivmaßnahmen in der rechten Szene informiert. Aus einem Vermerk des Bundesinnenministeriums:[71]

    > *Nach Rücksprache (...) stützen sich die "ermittlungstaktischen Gründe" vermutlich auf die Befürchtung, die Verfassungsschutzbehörden würden ihre Quellen über bevorstehende Exekutivmaßnahmen informieren.*

  - 2008 wurden Ermittlungen gegen den Neonazi Sebastian Seemann eingestellt. Er baute das verbotene *Blood and Honour* Netzwerk auf und war im schwerkriminellen Millieu aktiv (Drogen- und Waffenhandel). Der Verfassungsschutz warnte ihn vor Exekutivmaßnahmen. Mitarbeiter des Verfassungsschutzes wurden daraufhin wegen Geheimnisverrats und Strafvereitelung im Amt angeklagt. Auf Veranlassung des Innenministers Dr. Ingo Wolff wurden die Anklagen eingestellt.[72]

Das ist seit mehreren Jahren bekannt. Konsequenzen? Nur die Landesregierung in Thüringen unter Führung von B. Ramelow (Linke) geht den entgegengesetzten Weg und schafft die V-Leute des BfV ab, weil das V-Leute-System nicht die Sicherheit erhöht, sondern die Demokratie gefährdet.[73] Der Bundesinnenminister möchte die Strafheit für staatlichen Spitzel erweitern, damit sie stärker an szenetypischen Aktionen teilnehmen können (z.B Brandanschläge auf Unterkünfte für Asylbewerber u.ä.)

---

[68] https://www.heise.de/tp/blogs/8/151641
[69] https://www.heise.de/tp/artikel/31/31120/1.html
[70] http://www.spiegel.de/panorama/justiz/verfassungsschutz-soll-rechte-v-leute-vor-strafverfolgung-geschuetzt-haben-a-865154.html
[71] https://www.taz.de/Neonazi-Ermittlungen/!103340/
[72] http://www.nadir.org/nadir/initiativ/azzoncao/donazi3.html
[73] http://www.taz.de/Verfassungsschutz-in-Thueringen/!156778/

Strategie der Spannung

> *Geheimdienste ... sind nach wie vor die große Unbekannte in der Entstehung und Entwicklung des Terrorismus, des bundesdeutschen ebenso wie des mit ihm verflochtenen internationalen Terrorismus.* (W. Kraushaar)

Viele Terrorgruppen in Deutschland wurden von V-Leuten des Verfassungsschutzes aufgebaut. Strafrechtliche Konsequenzen haben diese Terroristen nicht zu befürchten, wir sollten aber die sich daraus ergebende Beeinflussung der Gesetzgebung fürchten:

- Der V-Mann Melvüt Kar hat drei Terrorzellen aufgebaut und an die Behörden verraten. Melvüt Kar wurde in Deutschland nie angeklagt und lebt unbehelligt in Istanbul in der Türkei.[74]
  - Die erste Terrorzelle mit Mutlu A., Mohamed El-A. und Issam El-S wurde am 17. Februar 2003 von der GSG9 verhaftet und am gleichen Tag aus Mangel an Beweisen wieder freigelassen.
  - Die Verhaftung der zweiten Terrorzelle mit Dzavid B., Nedzad B., Ahmed H., Bekim T. und Blerim T. wurde von den Medien weitgehend ignoriert.
  - Der größte Coup von Mevlüt Kar war die Sauerländer Terrorzelle, die von ihm für die Vorbereitung gigantischer Terroranschläge mit Sprengzündern usw. versorgt wurde

  Melvüt Kar soll vom Verfassungsschutz nie aktiv zur Gründung von Terrorgruppen gedrängt worden sein. Er soll selbstständig gehandelt haben, um seinen Wert als V-Mann und damit seine Bezahlung zu verbessern. Das BfV hat das Treiben toleriert und gedeckt und vor allem die Sauerland Terrorzelle medial für die Schaffung einer Atmosphäre der Spannung (Terrorgefahr!) genutzt.

- Ein weiterer V-Mann des Verfassungsschutzes in der islamistischen Szene war Yehia Yousif, der mittlerweile in Saudi-Arabien lebt und auch eine Schlüsselrolle in der Radikalisierung der Sauerland Gruppe spielte. Yousif hat wesentlich zum Erstarken salafistischer Gruppen in Deutschland beigetragen.[75]

- Die *Globale Islamische Medienfront* (GIMF) drohte 2007 in Videos mit Terroranschlägen in Deutschland. Im Gerichtsverfahren gegen Mitglieder der GIMF kam heraus, dass der Anführer dieser Gruppe ein V-Mann des Verfassungsschutzes war. Irfan Peci soll monatlich 2.500 - 3.000 Euro vom Verfassungsschutz erhalten haben. Außerdem finazierte das BfV die Ausbildung an Waffen in einem Terrorcamp in Bosnien und deckte Straftaten von Peci. Gegen den V-Mann wurde ebenfalls keine Anklage erhoben.[76]

  Im Gegensatz zu M. Kar wurde I. Peci aktiv vom Verfassungsschutz geführt und hat seine Terrorgruppe unter Anleitung des BfV aufgebaut.

[74] https://www.heise.de/tp/artikel/35/35986/1.html
[75] https://www.heise.de/tp/blogs/8/150854
[76] https://www.heise.de/tp/blogs/8/150854

Ohne die zweifelhafte Rolle der V-Leute würden wir ruhiger leben und viele Sicherheitsgesetze wären nicht durchsetzbar gewesen.

Schutz gegen Wirtschaftsspionage???

Der Verfassungsschutz warnt gelegentlich vor Wirtschaftsspionage aus Russland und China. Das ist wenig originell, dafür brauchen wir keinen Geheimdienst. Gegenüber unseren westlichen Verbündeten, insbesondere gegenüber der US-amerikanischen Wirtschaftsspionage gegen deutsche Unternehmen, stellt man sich blind. Verfassungschutzpräsident Maaßen ließ sich im Rahmen des NSA-Skandal zu folgendem Statement hinreißen:

> *Tatsächlich wurde bis zum heutigen Tage in ganz Europa kein einziger Fall amerikanischer oder britischer Wirtschaftsspionage nachgewiesen.*[77]

Ein anonymer Mitarbeiter des Verfassungsschutzes sagte dagegen bereits 1998 in der Sendung PlusMinus des WDR:

> *Mir sind über 50 solcher Fälle von Wirtschaftsspionage bekannt. Wenn wir auf solche Aktivitäten stoßen, werden wir von unseren Vorgesetzten zurückgepfiffen. Wir dürfen unsere Erkenntnisse meist weder an den Staatsanwalt noch an die betroffenen Firmen weitergeben. Aus Rücksicht auf unsere Verbündeten.*[78]

Den spektakulären Fall Enercon[79] findet man leicht, wenn man bei einer Suchmaschine der Wahl die passenden Suchbegriffe nach Wirtschaftsspionage der NSA in Deutschland eingibt, für Hr. Maaßen ist das wohl zuviel verlangt.

Auch dem BND waren die Ambitionen der NSA zur Wirtschaftsspionage seit Jahren bekannt, wie der Ex-General D. Urmann vor dem Untersuchungsschuss des Bundestages erklärte.[80] Verfassungschutzpräsident Maaßen wurde nicht darüber informiert? Schwer vorstellbar.

NSU-Skandal

Der NSU-Skandal gilt als der größte Geheimdienstskandal der BRD. 10 Jahre zog ein rechtsradikales Trio mordend durch Deutschland. Der Verfassungsschutz erhielt viele Hinweise von V-Leuten, die nicht an die Polizei weitergegeben wurden. Nach Schätzungen waren bis zu 25 V-Leute des BfV in der Umgebung des NSU tätig. Die genaue Zahl ist nicht rekonstruierbar. Die meisten Akten über den NSU und über Tarnfirmen des BfV im rechtsradikalen Milieu wurden vernichtet, als das BKA die Ermittlungen übernahm. Sieben Zeugen aus dem Umfeld des NSU sind überraschend verstorben, bevor man ihre Aussagen aufnehmen konnte.

- Der V-Mann Florian H.[81] verbrannte beispielsweise in seinem Auto wenige Stunden bevor das BKA ihn als Zeuge vernehmen wollte. Die Poli-

[77] https://heise.de/-1943975
[78] http://web.archive.org/web/20001208141100/http://www.wdr.de/tv/plusminus/archiv/980414/lauschangr.html
[79] https://de.wikipedia.org/wiki/Enercon
[80] https://heise.de/-2569294
[81] http://www.berliner-zeitung.de/nsu-prozess/nsu-prozess-wichtiger-zeuge-im-auto-verbrannt,11151296,24474928.html

zei diagnostizierte Selbstmord aus Liebeskummer, obwohl seine Freundin nichts von Liebeskummer wusste und es keinen Abschiedsbrief gab. Die Familie des V-Manns erhebt schwere Vorwürfe wegen schlampiger Ermittlungen bei der Polizei.[82]

- Der wertvolle V-Mann Thomas R. lieferte dem BfV viele Informationen über den NSU. Vor Gericht verweigerte er die Aussage. Er starb überraschend an einem Zucker-Schock (Diagnose: nicht behandelte schwere Diabetis), bevor er in Beugehaft genommern werden konnte, um eine Aussage zu erzwingen.[83]

Welche Konsquenzen haben sich drei Jahre nach der Aufdeckung des NSU-Skandals für den Verfassungsschutz ergeben?

- 47 Mitarbeiter der Abteilung Rechtsextremismus wurden befördert. Drei Mitarbeiter, die direkt für die Aktenvernichtung verantwortlich waren, wurde auf andere Posten versetzt ohne dienstrechtliche oder strafrechtliche Konsequenzen.[84]

- Am 3. Jahrestag der Aufdeckung des NSU-Skandals besuchte Merkel offiziell das Bundesamt für Verfassungsschutz. Die Wahl dieses Datums für einen offiziellen Besuch ist ein politisches Statement.[85]

- Der Etat des Bundesamtes für Verfassungsschutz wurde um 21 Mio. Euro auf 231 Mio. Euro erhöht.[86]

Aktive Rolle bei neuen Überwachungsgesetzen

Bei vielen Überwachungsgesetzen ist das BfV eine treibende Kraft. Geheimdienste sind zweifellos die Hauptnutznießer der vollständigen Protokollierung unseres Kommunikationsverhaltens.

Die Fernmeldeverkehr-Überwachungsverordnung (FÜV) wurde 1995 auf Initiative des Verfassungschutzes beschlossen. Die Verordnung wurde 2002 durch die TKÜV ersetzt und verpflichtete Telekommunikationsanbieter zur Kooperation mit Strafverfolgung und Geheimdiensten.

Die Vorratsdatenspeicherung brachte 2009 so gut wie keine Verbesserungen bei der Aufklärung von Straftaten im Internet. Trotzdem forciert der Verfassungsschutz im Hintergrund weiterhin die Einführung der VDS (neudeutsch: Mindestspeicherfrist). Nachdem die VDS schon 2002 als nicht vereinbar mit der Verfassung vom Bundestag abgelehnt wurde und auf EU-Ebene offenbar nicht durchsetzbar ist, beteiligte sich der Verfassungschutz 2012 aktiv an der

[82] http://www.stuttgarter-zeitung.de/inhalt.nsu-untersuchungsausschuss-vorwuerfe-nach-ominoeser-selbsttoetung.a05cce3a-60a5-4d68-9b24-7a6693123002.html
[83] http://www.sueddeutsche.de/politik/nsu-prozess-tod-von-v-mann-corelli-wirft-fragen-auf-1.1940178
[84] http://www.taz.de/Verfassungsschutz-und-NSU/!150371/
[85] https://www.heise.de/tp/news/Der-NSU-und-der-Verfassungsschutz-Dinge-von-gestern-2440935.html
[86] https://www.bundestag.de/dokumente/textarchiv/2014/kw48_ak_inneres/341274

Formulierung einer internationalen Richtline zur verpflichtenden Vorratsdatenspeicherung im Rahmen der UNODC, die allerdings ebenfalls nicht verbindlich umgesetzt wurde.[87].

Zukünftige Schwerpunkte des Geheimdienstes

Das Bundesamt für Verfassungsschutz soll in den kommenden Jahren zu einer kleinen Mini-NSA werden. Die Kompetenzen und Fähigkeiten zur Überwachung im Internet soll massiv ausgebaut werden, wie Netzpolitik.org[88] anhand vertraulicher Unterlagen berichtete. Die neu zu schaffende Abteilung *Erweiterte Fachunterstützung Internet* (EFI, 75 neue Mitarbeiter) soll Soziale Netzwerke, Foren u.ä. automatisiert überwachen und dabei überwiegend unterhalb der Schwelle des G10-Gesetzes agieren, also ohne parlamentariche Kontrolle durch die G10-Kommision. Außerdem sollen neue Analysemethoden geschaffen werden, um anhand von Metadaten bessere Bewegungs- und Kommunikationsprofile zu erstellen.

Der Abgeordnete C. Ströbele bezeichnte die Aufgabenstellung für die Abteilung EFI als illegal und nicht mit der Verfassung vereinbar.[89]

Überwachung politischer Aktivisten

Der Verfassungsschutz entwickelt sich zu einem Geheimdienst zur Überwachung von politischen Aktivisten und unliebsamen Abgeordneten.

- R. Gössler: 38 Jahre zu Unrecht vom Verfassungschutz überwacht [90]
- Verfassungsschutz in Bayern überwacht die linke Szene [91]
- Überwachung einer linken Gruppe durch Verfassungsschutz [92]
- Verfassungsschutz bespitzelt linke Abgeordnete [93]
- Gegner von Stuttgart21 vom Verfassungsschutz überwacht [94]
- Kultur- und Jugendprojekt Conne Island vom BfV überwacht [95]
- mg-Überwachung durch den Verfassungsschutz war illegal [96]
- Ohne demokratische Kontrolle (BfV in Bayern) [97]

[87] https://netzpolitik.org/2012/uno-bericht-der-kampf-gegen-terroristen-beginnt-im-internet-mit-vorratsdatenspeicherung-und-identifizierungspflicht/
[88] https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/
[89] http://www.stroebele-online.de/bundestag/anfragen/8305504.html
[90] https://heise.de/-217246
[91] https://www.heise.de/tp/artikel/35/35942/1.html
[92] https://www.heise.de/tp/blogs/8/151499
[93] https://www.heise.de/tp/artikel/36/36316/1.html
[94] http://www.bei-abriss-aufstand.de/2012/02/25/
[95] http://www.bei-abriss-aufstand.de/2012/02/25/
[96] http://www.l-iz.de/Politik/Sachsen/2014/05/Verfassungsschutz-raeumt-Bespitzelung-von-Conne-ein-55195.html
[97] https://www.heise.de/tp/artikel/35/35942/1.html

2.13 Ich habe doch nichts zu verbergen

Dies Argument hört man oft. Haben wir wirklich nichts zu verbergen? Einige Beispiele für spezielle Detektoren und Einzelbeispiele sollen exemplarisch zeigen, wie tief Big Data in unser Leben eingreift und wie willkürlich gesammelte Daten unser Leben gravierend beeinflussen können:

Erkennung einer neuen Liebesbeziehung

Der Beginn einer neuen Liebe oder einer erotischen Affäre ist anhand der Änderungen im Kommunikationsverhalten gut erkennbar. Big Data Analysten nennen die typischen Muster *Balzverhalten*. Alle Player auf dem Gebiet Datenanalyse (kommerzielle Datensammler, Anbieter von Software zur Mitarbeiterüberwachung, Geheimdienste) haben passende Detektoren zur Erkennung von *Balzverhalten* entwickelt.

- Marketingexperten haben herausgefunden, dass man sich in dieser Situation leichter zum Wechsel von Marken bewegen lässt und mehr Geld ausgibt.
- Headhunter wissen, dass man Menschen in dieser Situation leichter zu beruflichen Veränderungen bewegen kann.
- Personalmanager großer Firmen interessieren sich für die Auswirkungen auf die Produktivität bei Affären innerhalb der Firma.
- Geheimdienste interessieren sich für die Erpressbarkeit von Target Personen.

Arbeitslos?

Unser Smartphone liefert die aktuelle Position des Nutzers an viele Trackingdienste. Außerdem verraten Postings bei Twitter oder Facebook unseren Aufenthaltsort.

In der Regel sind wir Nachts zuhause und an Werktagen tagsüber an unserem Arbeitsplatz. Was kann man schlußfolgern, wenn sich dieses Verhalten ändert und man auch tagsüber über einen längeren Zeitraum zuhause bleibt in Kombination mit einem sparsameren Konsumverhalten bei Online Einkäufen oder Offline Einkäufen mit Rabattkarten bzw. Kreditkarten? Welchen Einfluss hat das auf unsere Kreditwürdigkeit?

Unzufrieden mit dem Job?

Vorreiter auf diesem Gebiet war Google. Schon 2010 protzte Google damit, dass sie im Rahmen der Mitarbeiterüberwachung den Wunsch nach beruflicher Veränderung schneller erkennen können, als der betroffene Mitarbieter sich selbst darüber im Klaren ist. Inzwischen nutzen auch andere Firmen diese Überwachung. Personalchefs können auf einen solchen computergenerierten Verdacht unterschiedlich reagieren. Einarbeitung eines Nachfolgers und Entlassung des verdächtigen Mitarbeiters ist eine Möglichkeit.

L. Reppesgaard hat im Rahmen eines Selbstversuches mehrere E-Mails von seinem GMail Account versendet mit kritischen Bemerkungen zu seinem Arbeitsverhältnis. Unmittelbar darauf konnte er Veränderungen in der personalisierten Werbung registrieren, die plötzlich auf Headhunter und kommerzielle Jobbörsen hinwies.

Kein Studienplatz?

In Großbritannien werden Studienbewerber für bestimmte Fachrichtung geheimdienstlich überprüft. 739 Bewerber wurde bereits abgelehnt, weil aufgrund dubioser Datensammlungen der Geheimdienste befürchtet wurde, dass die Bewerber zu Terroristen werden und die im Studium erworbenen Kenntnisse zur Herstellung von Massenvernichtungswaffen nutzen könnten. Die geheimdienstlichen Gesinnungs-Prüfungen sollen zukünftig ausgeweitet werden.[98]

Einzelbeispiele

- Emma L. hatte sich auf dem Dating-Portal OkCupid zu einem Treffen verabredet. Das Date war ein Reinfall (kommt manchmal vor). Wenig später wurde ihr der Dating-Partner von Facebook als Freund empfohlen, in der *People You May Know* Section. Maria L. wurden ihre Tinder-Dates von Facebook als Freunde empfohlen. Es gibt auf Twitter noch viele weitere Beispiele für diese seltsamen Facebook Empfehlungen.[99]

  Weder OkCupid nich Tinder geben Daten an Facebook weiter. Die Empfehlungen für Freunde werden anhand der Geolocation (*zur gleichen Zeit am gleichen Ort*) und aufgrund ähnlicher Interessen (*Dating-Webseite besucht*) ermittelt. Daraus könnten sich auch unangenehme Folgen ergeben, wie Netzpolitik.org an Beispielen zeigt.[100]

- Target ist einer der größte Discounter in den USA. Eines Tages stürmte ein wütender Vater in eine Filiale und beschwert sich, dass seine minderjährige Tochter Rabattmarken für Babysachen erhalten hat. Später musste der Vater kleinlaut zugegeben, dass seine Tochter wirklich schwanger war, er selbst aber nichts davon wusste. Target hatte die Schwangerschaft der minderjährigen Tochter an den kleinen Änderungen im Kaufverhalten erkannt.[101]

- Im Rahmen der Zulässigkeitsprüfung für Piloten wurde Herr J. Schreiber mit den vom Verfassungsschutz gesammelten Fakten konfrontiert [102]:

  1. Er wurde 1994 auf einer Demonstration kontrolliert. Er wurde nicht angezeigt, angeklagt oder einer Straftat verdächtigt, sondern nur als Teilnehmer registriert.

[98] https://www.heise.de/tp/artikel/44/44538/1.html
[99] https://twitter.com/search?q=facebook%20suggest%20tinder
[100] https://netzpolitik.org/2016/facebook-nutzt-standort-fuer-freundesvorschlaege/
[101] http://www.tagebau.com/?p=197
[102] http://www.pilotundflugzeug.de/artikel/2006-02-10/Spitzelstaat

2. Offensichtlich wurde daraufhin sein Bekanntenkreis durchleuchtet.
3. Als Geschäftsführer einer GmbH für Softwareentwicklung habe er eine vorbestrafte Person beschäftig. Er sollte erklären, welche Beziehung er zu dieser Person habe.
4. Laut Einschätzung des Verfassungsschutzes neige er zu politischem Extremismus, da er einen Bauwagen besitzt. Bei dem sogenannten *Bauwagen* handelt es sich um einen Allrad-LKW, den Herr S. für Reisen nutzt (z.B. in die Sahara).

Für Herrn S. ging die Sache gut aus. In einer Stellungnahme konnte er die in der Akte gesammelten Punkte erklären. In der Regel wird uns die Gelegenheit zu einer Stellungnahme jedoch nicht eingeräumt. Es werden Entscheidungen getroffen und wir haben keine Ahnung, welche Daten dabei eine Rolle spielten.

- Ein junger Mann meldet sich freiwillig zur Bundeswehr. Mit sechs Jahren war er kurzzeitig in therapheutischer Behandlung, mit vierzehn hatte er etwas gekifft. Seine besorgte Mutter ging mit ihm zur Drogenberatung. In den folgenden Jahren gab es keine Drogenprobleme. Von der Bundeswehr erhält er eine Ablehnung, da er ja mit sechs Jahren eine Psychotherapie durchführen musste und Drogenprobleme gehabt hätte. [103].
- Kollateralschäden: Ein großer deutscher Provider liefert falsche Kommunikationsdaten ans BKA. Der zu Unrecht Beschuldigte erlebt das volle Programm: Hausdurchsuchung, Beschlagnahme der Rechner, Verhöre und sicher nicht sehr lustige Gespräche im Familienkreis. Die persönlichen und wirtschaftlichen Folgen sind schwer zu beziffern [104].

  Noch krasser ist das Ergebnis der *Operation Ore* in Großbritannien. Einige Tausend Personen wurden wegen Konsums von Kinderpornografie angeklagt. Acht Jahre später stellte sich heraus, dass die meisten Betroffen zu unrecht verurteilt wurden, weil sie Opfer von Kreditkarten Betrug waren. 39 Menschen hatten Selbstmord begangen, da ihnen alles genommen wurde. [105].
- "Leimspur des BKA": Wie schnell man in das Visier der Fahnder des BKA geraten kann, zeigt ein Artikel bei Zeit-Online. Die Webseite des BKA zur Gruppe "mg" ist ein Honeypot, der dazu diente, weitere Sympathisanten zu identifizieren. Die Bundesanwaltschaft verteidigt die Maßnahme als legale Fahndungsmethode.

  Mit dem im Juni 2009 beschlossenen BSI-Gesetz übernimmt die Behörde die Aufzeichnung und unbegrenzte Speicherung personenbezogener Nutzerinformationen wie IP-Adressen, die bei der Online-Kommunikation zwischen Bürgern und Verwaltungseinrichtungen des Bundes anfallen. Ich kann daraus nur den Schluss ziehen, diese und ähnliche Angebote in Zukunft ausschließlich mit Anonymisierungsdiensten zu nutzen.

[103] http://blog.kairaven.de/archives/998-Datenstigmaanekdote.html
[104] http://www.lawblog.de/index.php/archives/2008/03/11/
[105] http://en.wikipedia.org/wiki/Operation_Ore

Nicht immer treten die (repressiven) Folgen staatlicher Sammelwut für die Betroffenen so deutlich hervor. In der Regel werden Entscheidungen über uns getroffen, ohne uns zu benachrichtigen. Wir bezeichnen die (repressiven) Folgen dann als Schicksal.

Politische Aktivisten

Wer sich politisch engagiert und auf gerne vertuschte Mißstände hinweist, hat besonders unter der Sammelwut staatlicher Stellen zu leiden. Einige deutsche Beispiele:

1. Erich Schmidt-Eenboom veröffentliche 1994 als Publizist und Friedensforscher ein Buch über den BND. In den folgenden Monaten wurden er und seine Mitarbeiter vom BND ohne rechtliche Grundlage intensiv überwacht, um die Kontaktpersonen zu ermitteln. Ein Interview unter dem Titel *"Sie beschatteten mich sogar in der Sauna"* [106] gibt es bei SPON.

2. Fahndung zur Abschreckung: In Vorbereitung des G8-Gipfels in Heiligendamm veranstaltete die Polizei am 9. Mai 2007 eine Großrazzia. Dabei wurden bei Globalisierungsgegnern Rechner, Server und Materialien beschlagnahmt. Die Infrastruktur zur Organisation der Proteste wurde nachhaltig geschädigt. Wenige Tage nach der Aktion wurde ein Peilsender des BKA am Auto eines Protestlers gefunden. Um die präventiven Maßnahmen zu rechtfertigen, wurden die Protestler als terroristische Vereinigung eingestuft. Das Netzwerk Attac konnte 1,5 Jahre später vor Gericht erreichen, dass diese Einstufung unrechtmäßig war. Das Ziel, die Organisation der Proteste zu behindern, wurde jedoch erreicht.

3. Dr. Rolf Gössner ist Rechtsanwalt, Vizepräsident der Internationalen Liga für Menschenrechte, Mitherausgeber des Grundrechte-Reports, Vizepräsident und Jury-Mitglied bei den Big Brother Awards. Er wurde vom Verfassungsschutz 38 Jahre lang überwacht. Obwohl das Verwaltungsgericht Köln bereits urteilte, dass der Verfassungsschutz für den gesamten Bespitzelungszeitraum Einblick in die Akten gewähren muss, wird dieses Urteil mit Hilfe der Regierung ignoriert. Es werden Sicherheitsinteressen vorgeschoben!

Mit dem Aufbau der "neuen Sicherheitsarchitektur" bedeutet eine Überwachung nicht nur, dass der direkt Betroffene überwacht wird. Es werden Bekannte und Freunde aus dem persönlichen Umfeld einbezogen. Sie werden in der AntiTerrorDatei gespeichert, auch ihre Kommunikation kann überwacht werden, es ist sogar möglich, Wanzen in den Wohnungen der Freunde zu installieren.

[106] http://www.spiegel.de/politik/deutschland/0,1518,384374,00.html

Kapitel 3

Digitales Aikido

Die folgende grobe Übersicht soll die Orientierung im Dschungel der nachfolgend beschriebenen Möglichkeiten etwas erleichtern.

- **Einsteiger:** Datensammler nutzen verschiedene Möglichkeiten, Informationen über die Nutzer zu generieren. Die Wiedererkennung des Surfers bei der Nutzung verschiedener Dienste kann mit einfachen Mitteln erschwert werden. Datensammler meiden und Alternativen nutzen, Cookies und JavaScript kontrollieren, Werbung filtern, SSL-verschlüsselte Verbindungen nutzen, E-Mail Client sicher konfigurieren...
- **1. Grad:** Persönliche Daten und Inhalte der Kommunikation werden verschlüsselt. Das verwehrt unbefugten Dritten, Kenntnis von persönlichen Daten zu erlangen. Festplatte und Backups verschlüsseln mit Truecrypt, dm-crypt oder FileVault, E-Mails verschlüsseln mit GnuPG oder S/MIME, Instant Messaging mit OTR oder OMEMO...
- **2. Grad:** Anhand der IP-Adresse ist ein Nutzer eindeutig identifizierbar. Anonymiserungsdienste wie Tor Onion Router bieten eine dem realen Leben vergleichbare Anonymität. Remailer bieten die Möglichkeit, den Absender einer E-Mail zu verschleiern.
- **3. Grad:** Eine noch höhere Anonymität bieten anonyme Peer-2-Peer Netze wie z.B. das *Invisible Internet Projekt* (I2P) oder das *GNUnet*. Eine dezentrale und vollständig verschlüsselte Infrastruktur verbirgt die Inhalte der Kommunikation und wer welchen Dienst nutzt. Auch Anbieter von Informationen sind in diesen Netzen anonym.

Die einzelnen Level bauen aufeinander auf! Es macht wenig Sinn, die IP-Adresse zu verschleiern, wenn man anhand von Cookies eindeutig identifizierbar ist. Auch die Versendung einer anonymen E-Mail ist in der Regel verschlüsselt sinnvoller.

3.1 Nachdenken

Eine Graduierung in den Kampfsportarten ist keine Garantie, dass man sich im realen Leben erfolgreich gegen einen Angreifer zur Wehr setzen wird.

Ähnlich verhält es sich mit dem *Digitalen Aikido*. Es ist weniger wichtig, ob man gelegentlich eine E-Mail verschlüsselt oder einmal pro Woche Anonymisierungsdienste nutzt. Entscheidend ist ein konsequentes, datensparsames Verhalten.

Ein kleines Beispiel soll zum Nachdenken anregen. Es ist keinesfalls umfassend oder vollständig. Ausgangspunkt ist eine reale Person P mit Namen, Geburtsdatum, Wohnanschrift, Fahrerlaubnis, Kontoverbindung. . .).

Im Internet verwendet diese Person verschiedene Online-Identitäten:

1. Facebook Account (es könnte auch Xing oder ein ...VZ sein).
2. Eine E-Mail Adresse mit dem realen Namen.
3. Eine anonyme/pseudonyme E-Mail Adresse bei einem ausländischen Provider.
4. Pseudonyme in verschiedenen Foren, die unter Verwendung der anonymen E-Mail Adresse angelegt wurden.
5. Für Kommentare in Blogs verwendet die Person meist ein einheitliches Pseudonym, um sich Anerkennung und Reputation zu erarbeiten. (Ohne Reputation könnte das soziale Gefüge des Web 2.0 nicht funktionieren.)

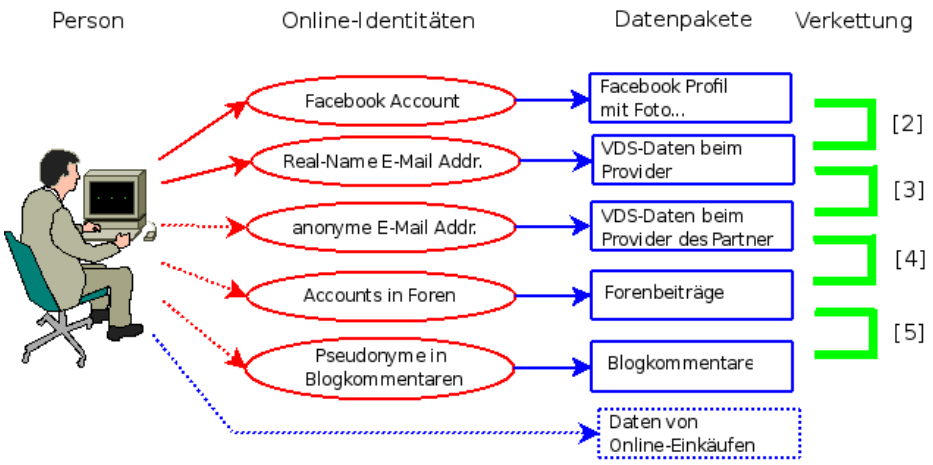


Abbildung 3.1: Datenverkettung

Mit diesen Online-Identitäten sind verschiedene Datenpakete verknüpft, die irgendwo gespeichert und vielleicht nicht immer öffentlich zugänglich sind. Um übersichtlich zu bleiben nur eine minimale Auswahl:

- Das Facebook Profil enthält umfangreiche Daten: Fotos, Freundeskreis. . .
- Bei der Nutzung von vielen Webdiensten fallen kleine Datenkrümel an. Auch E-Mails werden von den Datensammlern ausgewertet. Die IP-Adresse des Absenders im Header der E-Mails kann mit anderen Einträgen von Cookies oder User-Tracking-Systemen zeitlich korreliert werden

und so können den Surf-Profilen die Mail-Adressen und reale Namen zugeordnet werden.

- Von dem anonymen E-Mail Postfach findet man Daten bei den Empfängern der E-Mails. (Google has most of my emails because it has all of yours.) Auch diese Datenpakete enthalten einen Zeitstempel sowie oft die IP-Adresse des Absenders. Durch zeitliche Korrelation kann das anonymen E-Mail Postfach mit dem Real-Name Postfach und dem Surf-Profil verknüpft werden.

- In Foren und Blogs findet man Postings und Kommentare, häufig mit den gleichen Pseudonymen, die auch für die E-Mail Adressen verwendet werden.

- Online-Einkäufe erforden die Angaben zur Kontoverbindung und einer Lieferadresse, die der Person zugeordnet werden können.

Verkettung der Informationen und Datenpäckchen

Die verschiedenen Datenpakete können auf vielfältige Art verknüpft werden. Diese Datenverkettung ist eine neue Qualität für Angriffe auf die Privatsphäre, die unterschätzt wird.

1. Online Communities wie Facebook bieten viele Möglichkeiten. Neben der Auswertung von Freundschaftsbeziehungen gibt es auch viele Fotos. Dieser Datenpool ist schon sehr umfangreich:

   - Wirtschaftswissenschaftler haben eine Methode vorgestellt, um Meinungsmacher und kreative Köpfe in Online-Communities zu identifizieren [1].
   - MIT-Studenten erkennen homosexuelle Neigungen ihrer Kommilitonen anhand der Informationen über Freundschaften in den Facebook-Profilen [2].
   - Der Grünen-Vorsitzende Özdemir pflegte eine Freundschaft mit dem Intensivstraftäter Muhlis Ari, ist in seinem Facebook Profil erkennbar [3].

2. Dem Facebook Profil kann man durch Kombination mit anderen Datenkrümeln den realen Namen und die meisten genutzten E-Mail Adressen zuordnen. Die Firma Rapleaf ist z.B. darauf spezialisiert. Auch pseudonyme Facebook Accounts können deanonymisiert werden.

3. Durch Analyse der im Rahmen der VDS gespeicherten IP-Adressen können bei zeitlicher Übereinstimmung beide E-Mail Adressen der gleichen Person zugeordnet werden. Ein einzelner passender Datensatz reicht aus. (Wenn nicht konsequent Anonymisierungsdienste für das anonyme Postfach verwendet werden.)

[1] http://www.heise.de/tp/r4/artikel/31/31691/1.html
[2] http://www.heise.de/tp/r4/artikel/31/31181/1.html
[3] http://www.heise.de/tp/r4/artikel/32/32138/1.html

4. Die Verbindung zwischen anonymer E-Mail Adresse und Foren Account ergibt sich durch die Nutzung der E-Mail Adresse bei Anmeldung.

5. Durch Vergleiche von Aussagen und Wortwahl lassen sich Korrelationen zwischen verschiedenen Nicknamen in Foren und Blogs herstellen. Dem Autor sind solche Korrelationen schon mehrfach offensichtlich ins Auge gesprungen und konnten durch Nachfrage verifiziert werden.

6. Durch Datenschutzpannen können Informationen über Online-Einkäufe mit anderen Daten verknüpft werden. Dabei schützt es auch nicht, wenn man sich auf das Gütesiegel des TÜV Süd verlässt und bei einem Händler einkauft, der bisher nicht negativ aufgefallen ist. Eine kleine Zusammenfassung vom 29.10.09 bis 04.11.09:

   - Die Bücher der Anderen (500.000 Rechnungen online einsehbar [4])
   - Die Libris Shops (Zugang zu Bestellungen von 1000 Buchshops [5])
   - Sparkassen-Shops (350.000 Rechnung online einsehbar [6])
   - Acht Mio. Adressen von Quelle-Kunden sollen verkauft werden [7]

   Eine reichhaltige Quelle für Datensammler, die Profile ihrer Zielpersonen vervollständigen wollen oder nach potentiellen Zielpersonen rastern.

Durch die Verkettung der Datenpäckchen konnten in dem fiktiven Beispiel alle Online Identitäten de-anonymsiert werden. Für den Sammler, der diese Datensammlung in der Hand hält, ergibt sich ein komplexes Persönlichkeitsbild der Person P. Diese Datensammlung könnte das Leben von P in vielerlei Hinsicht beeinflussen, ohne dass dem Betroffenen klar wird, dass hinter scheinbar zufälligen Ereignissen ohne Zusammenhang bewusste Entscheidungen stehen.

- Die Datensammlungen werden mit kommerziellen Zielen ausgewertet, um uns zu manipulieren und Kaufentscheidungen zu beeinflussen.

- Personalabteilungen rastern routinemäßig das Internet nach Informationen über Bewerber. Dabei ist Google nur ein erster Ansatzpunkt. Bessere Ergebnisse liefern Personensuchmaschinen und soziale Netzwerke. Ein kurzer Auszug aus einem realen Bewerbungsgespräch:

  - Personalchef: *Es stört Sie sicher nicht, dass hier geraucht wird. Sie rauchen ja ebenfalls.*
  - Bewerber: *Woher wissen Sie das?*
  - Personalchef: *Die Fotos in ihrem Facebook-Profil ...*

  Qualifizierten Personalchefs ist dabei klar, dass eine kurze Recherche in Sozialen Netzen kein umfassendes Persönlichkeitsbild liefert. Die gefundenen Indizien können aber den Ausschlag für eine Ablehnung geben, wenn man als Frau gebrauchte Unterwäsche anbietet oder der Bewerber eine Nähe zur Gothic-Szene erkennen lässt.

[4] http://www.netzpolitik.org/2009/exklusiv-die-buecher-der-anderen
[5] http://www.netzpolitik.org/2009/exklusiv-die-libri-shops-der-anderen
[6] http://www.netzpolitik.org/2009/zugriff-auf-350-000-rechnungen-im-sparkasse-shop
[7] http://www.zeit.de/digital/datenschutz/2009-11/quelle-kundendaten-verkauf

- Von der israelischen Armee ist bekannt, dass sie die Profile in sozialen Netzen überprüfen, wenn Frauen den Wehrdienst aus religiösen Gründen verweigern. Zur Zeit verweigern in Israel 35% der Frauen den Wehrdienst. Anhand der sozialen Netze wird der Lebenswandel dieser Frauen überprüft. Es werden Urlaubsfotos in freizügiger Bekleidung gesucht oder Anhaltspunkte für Essen in einem nicht-koscheren Restaurant. Auch aktiv wird dabei gehandelt und Fake-Einladungen zu einer Party während des Sabbats verschickt.

- Firmen verschaffen sich unrechtmäßig Zugang zu Verbindungs- und Bankdaten, um ihre Mitarbeiter auszuforschen (z.B. Telekom- und Bahn-Skandal).

- Identitätsdiebstahl ist ein stark wachsendes Delikt. Kriminelle duchforsten das Web nach Informationen über reale Personen und nutzen diese Identitäten für Straftaten. Wie sich Datenmissbrauch anfühlt: Man wird plötzlich mit Mahnungen für nicht bezahlte Dienstleitungen überschüttet, die man nie in Anspruch genommen hat [8].

- Mit dem Projekt INDECT hat die EU ein Forschungsprojekt gestartet und mit 14,8 Mio Euro ausgestattet, um unsere Daten-Spuren für Geheimdienste zu erschließen.[9]

Ich habe doch nichts zu verbergen...

...oder habe ich nur zu wenig Fantasie, um mir die Möglichkeiten der Datensammler vorstellen, mein Leben zu beeinflussen?

3.2 Ein Beispiel

Das Seminar für angewandte Unsicherheit (SAU) hat ein sehr schönes Lehrbeispiel im Internet vorbereitet. Jeder kann nach Informationen dieser fiktiven Person selbst suchen und das Profil verifizieren. Es geht um folgende Person:

Name:	Fiona Flauderer
geboren:	17.06.1985
E-Mail:	fiona.flauderer@gmail.com
Status:	Studentin
Anschrift:	Dorthenstr. 17, 10995 Berlin

Diese Informationen könnte ein Personalchef einer Bewerbung entnehmen oder sie sind der Krankenkasse bekannt oder sie ist bei einer Demo aufgefallen... Eine kurze Suche bei Google und verschiedenen Personensuchmaschinen liefert nur sehr wenige Treffer, im Moment sind es 3 Treffer. Gleich wieder aufgeben?

Die moderne Studentin ist sozial vernetzt. Naheliegend ist es, die verschiedenen Netzwerke wie StudiVZ usw. nach F. abzusuchen. Bei Facebook wird

[8] http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung
[9] http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

man erstmals fündig. Es gibt ein Profil zu dieser Person mit Fotos, Interessen und (wichtig!) eine neue E-Mail Adresse:

goagirl17@ymail.com

Bezieht man diese Adresse in die Suche bei anderen Sozialen Netzwerken mit ein, wird man bei MySpace.com erneut fündig. Hier gibt es ein Profil mit dieser E-Mail Adresse und man findet den Twitter-Account von F. sowie ein weiteres Pseudonym:

flaudi85

Mit den beiden gefundenen Pseudonymen g.....17 und f.....85 kann man erneut bei Google suchen und die Ergebnisse mit den Informationen aus den Profilen zusammenfassen.

- g.....17 ist offenbar depressiv. Das verordnete Medikament deutet auf Angstzustände hin, wurde von der Patientin nicht genommen sondern ins Klo geworfen.
- Sie hat Probleme im Studium und will sich krankschreiben lassen, um an Prüfungen nicht teilnehmen zu müssen.
- Außerdem hat sie ein massives Alkoholproblem und beteiligt sich am *Syncron-Saufen* im Internet. Scheinbar ist sie auch vereinsamt.
- F. ist offenbar lesbisch, sie sucht nach einer Frau bei abgefuckt.de.
- F. ist im linksradikalen Spektrum aktiv. Sie hat an mehreren Demonstrationen teilgenommen und berichtet über Erfahrungen mit Hausdurchsuchungen. Möglicherweise ist das die Ursache für ihre Angstzustände.
- Öffentlich prangert sie in einem Diskussionsforum die Firma ihres Vaters an (wegen Ausspionierens von Mitarbeitern).
- Ihre linksgerichtete Grundhaltung wird durch öffentliche Unterstützung der Kampagne *Laut ficken gegen Rechts* unterstrichen.
- Von regelmäßiger Arbeit hält sie nicht viel.
- Die angebene Adresse ist falsch. F. wohnt in einer 11-Personen-WG in einem besetzten Haus in Alt-Moabit. Die WG sucht nach einem neuem Mitglied.
- Die Wunschliste bei Amazon und Fotos bei Flickr...

Würden sie als Personalchef diese fiktive Person einstellen?

Welche Ansatzpunkte ergäben sich für den Verfassungsschutz?

Was könnte zukünftig für die Krankenkasse interessant sein?

Was hätte F. tun können, um die Profilbildung zu vermeiden?

3.3 Schattenseiten der Anonymität

Auf den ersten Blick scheint Anonymität eine Lösung für fast alle beschriebenen Probleme zu sein. Anonymität verhindert das Tracking durch kommerzielle Datensammler, schützt die Privatsphäre vor neugierigen Blicken der Spanner, schränkt die Überwachungsmöglichkeiten der Geheimdienste ein, bietet Whistleblowern Schutz....

Neben den unbestreitbaren Vorteilen hat Anonymität aber auch Schattenseiten. Einige kleine Denkanstöße sollen zu einem verantwortungsbewussten Umgang mit Anonymität anregen, bevor der technische Teil beginnt.

Am Beispiel ANONYMOUS sieht man einige Nachteile deutlich. ANONYMOUS ist als Protestgruppe gegen Scientology gestartet und mit dem Einsatz der *low orbit ion canone* (LOIC) gegen Banken zur Unterstützung von Wikileaks bekannt geworden. Heute belauscht ANONYMOUS angeblich den E-Mail Verkehr der lettischen Botschaft und veröffentlicht selektiv belastende E-Mails von Klitschko. Oder war das der russische GRU im Rahmen der Propagandaschlacht um die Krim? Das Label ANONYMOUS kann heute jeder Hanswurst für beliebige Zwecke missbrauchen und die Bewegung diskreditieren.

Reputation, Vertrauen, Respekt und Verantwortung sind an Persönlichkeit gebunden. Dabei muss Persönlichkeit nicht unbedingt mit einem realen Namen verbunden sein. Reputation und Respekt kann man auch unter einem Pseudonym oder als eine Gruppe erwerben, wenn man die Verantwortung für seine Handlungen übernimmt.

Im Schutz der Anonymität muss man aber keine Verantwortung für sein Handeln übernehmen, da Fehlverhalten oder gesellschaftlich unerwünschte Handlungen nicht sanktioniert werden können. In einem Diskussionsforum kann man sich verbale Entgleisungen erlauben, ohne negative Reputation für seine Person fürchten zu müssen. Man verwendet in Zukunft einfach einen neuen anonymen Account und beginnt von vorn. Das habe ich schon öfters erlebt. Dieser Umgang mit Anonymität ohne Verantwortung stört im einfachen Fall nur. Es kann aber auch schwerere Auswirkungen haben.

Ein anonymer Schwarm vereinzelter Individuen kann sich zu einem Shitstorm zusammenfinden. Der Schwarm kann kurzzeitig viel Lärm produzieren ohne gesellschaftlichen Diskurs und wird dann wieder zerfallen. Er wird kein *Wir!* entwickeln und kann keine gemeinsamen Ziele verfolgen, die über einen kurzzeitigen Hype in den Medien hinaus gehen. Außerdem lassen sich Empörungswellen durch eine kritische Masse anonymer Sockenpuppen leicht manipulieren.

Ein Beispiel für den Konflikt zwischen Anonymität und Vertrauen:

1. Ich kann mir ganz anonym in meiner Einsiedlerzelle mit einem Anonymisierungsdienst bei YouPorn, RedTube, XHamster....
2. Oder ich kann eine Frau im Arm halten, die sich sehnsuchtsvoll an mich

drängt, ihre Haut spüren, das gegenseitige Begehren fühlen und eintauchen in einen Strudel der ....

Bei Variante 1) bleibt meine Anonymität gewahrt aber sie hinterlässt gähnende Leere und Einsamkeit. Variante 2) funktioniert nur mit gegenseitigem Vertrauen und Respekt. Um die Liebesbriefe in 2. gegen mitlesende, sabbernde Schlapphüte zu schützen, ist **jedes** Mittel zulässig, aber Kryptografie, TorBrowser, JonDonym usw. sind nur Werkzeuge und kein Selbstzweck.

Für ein soziales Zusammenleben und gemeinsame Ziele brauchen wir Vertrauen. Vertrauen kann missbraucht werden, man muss es nicht leichtfertig verschenken. Es ist aber wichtig, bei aller gebotenen Vorsicht, auch einen Weg zu finden, um gegenseitiges Vertrauen aufzubauen.

Das Beispiel kann man auf beliebige Gebiete übertragen. Es gilt für politische Aktivisten, die genug haben von der Demokratiesimulation und dem *Stillen Putsch* etwas entgegen setzen wollen. Und es gilt für Mitglieder im Kleintierzüchterverein, die in den Suchergebnissen bei Google nicht ständig Links für Kaninchenfutter finden wollen. Welche Werkzeuge angemessen sind, hängt von den konkreten Bedingungen ab.

3.4 Wirkungsvoller Einsatz von Kryptografie

Nach einer anerkannten Faustregel ist der wirkungsvolle Einsatz von Kryptografie von folgenden allgemeinen Faktoren abhängig:

- zu 10% hängt der Schutz von der eingesetzten Technik ab
- zu 60% beeinflusst das Wissen der Anwender über Möglichkeiten und Grenzen den wirkungsvollen Einsatz kryptografischer Verfahren
- zu 30% hängt die Wirksamkeit von der Disziplin der Anwender ab

Bevor es mit konkreten Anleitungen weiter geht, sollen einige allgemeine Gedanken zum Nachdenken über die Verwendung von Verschlüsselung anregen. Man kann natürlich einfach irgendwie beginnen, irgendwas zu verschlüsseln. Nachhaltigen und vor allem wirksamen Schutz gegen Überwachung und Datensammlung erreicht man damit aber nicht.

1. Kryptografie ist kein Selbstzweck sondern ein Hilfsmittel zum Schutz unserer Privatsphäre. Erste Voraussetzung für den wirksamen Einsatz von Kryptografie ist, dass eine Privatsphäre existiert, die geschützt werden kann. Dieser Bereich privater Lebensführung entsteht nicht zwangsläufig durch den Einsatz von Kryptografie, sondern muss zuerst **durch Verhalten** geschaffen werden.

   Beispiel: wenn man einem Bekannten eine verschlüsselte E-Mail mit einem Link zu der Sammlung von Urlaubsfotos bei Facebook schickt, dann gibt es keine Privatsphäre, die durch die Verschlüsselung der E-Mail geschützt werden könnte.

2. Wenn man einen Bereich gefunden oder festgelegt hat, den man gegen Datensammler und Überwachung schützen möchte, dann sollte die techn. Umsetzung des Schutzes vollständig und umfassend sein. Es ist nur wenig nachhaltig, wenn man gelegentlich eine verschlüsselte E-Mail schreibt und gleichzeitig zwei unverschlüsselte E-Mails mit dem gleichen Inhalt an anderer Empfänger (mit Google Accounts?) schickt.

   - Studien haben nachgewiesen, dass es ausreichend ist, in einer organisierten Gruppe nur 10-20% der Mitglieder zu überwachen, um über die Struktur der Gruppe und ihre wesentlichen Aktivitäten informiert zu sein.
   - Wenn man Anonymisierungsdienste zur Verwaltung von E-Mail Konten, für ein anonymes Blog, für digitale Identitäten oder zur Recherche zu sensiblen Themen nutzt, dann muss man sie in diesem Kontext immer nutzen. Anderenfalls könnten die Aktivitäten aus der Vergangenheit nachträglich deanonymisiert werden und für die Zukunft ist die Anonymität in diesem Kontext nicht mehr gegeben.
   - Schützenswerte, private Daten (was das ist, muss man selbst definieren) sollten immer verschlüsselt gespeichert und transportiert werden. Das betrifft nicht nur die Speicherung auf dem eigenen Rechner sondern auch alle Backups und jede Kopie bei Dritten. Wer private Dateien ohne zusätzliche Verschlüsselung via Skype verschickt, sollte sich darüber klar sein, dass Microsoft immer mitliest.

   Die Umsetzung dieser Anforderung erfordert in erster Linie Disziplin im Umgang mit den technischen Kommunikationsmitteln. *Schnell mal...* ist immer schlecht. Man kann in kleinen Schritten spielerisch beginnen. Dabei sollte man das Gesamtziel aber nicht aus den Augen verlieren.

3. Die meisten Protokolle zur verschlüsselten Kommunikation verwenden Public Key Verfahren (SSL/TLS, OpenPGP, OTR, SSH). Wenn man für hohe Anforderungen wirklich sicher sein will, dass nur der Kommunikationspartner (oder der Server bei SSL) die gesendeten Daten entschlüsseln kann, dann muss man den öffentliche Schlüssel der Gegenseite über einen sicheren, unabhängigen Kanal verifizieren.

   Ein universelles Verfahren für die Verifizierung von kryptografischen Schlüsseln ist der Vergleich des Fingerprint anhand veröffentlichter Werte. Über einen sicheren Kanal (z.B. persönliches Treffen) tauscht man die Fingerprints der public Keys aus und vergleicht sie später am eigenen Rechner mit den Fingerprints der tatsächlich verwendeten Schlüssel. Man kann die Fingerprints der eigenen Schlüssel auch veröffentlichen, um den Kommunikationspartnern die Verifikation zu ermöglichen.

   Alternativ könnte man sich den öffentlichen Schlüssel von vertrauenswürdigen Dritten beglaubigen lassen. (Wenn man einen vertrauenswürdigen(!) Dritten findet, der die Identität der Inhaber der kryptografischen Schlüssel wirklich geprüft hat.)

- OpenPGP bietet dafür das *Web of Trust*, dass die meisten Nutzer nicht ganz verstanden haben und das in der Praxis kaum eine Rolle spielt.
- Im SSL-Protokoll und bei S/MIME wurde das Konzept des *vertrauenswürdigen Dritten* durch Certification Authorities (CAs) pervertiert. CAs definieren sich mehr oder weniger selbst als vertrauenswürdig und sind der Meinung, eine einfachen E-Mail ist ein ausreichend sicherer Kanal für die Verifikation eines kryptografischen Schlüssels.

  Die laut Eigenwerbung größte CA ist Verisign. Seit 2002 ist bekannt, dass Verisign auch ein Global Player bei der Überwachungstechnik ist. Die Firma bietet Support für *Lawful SSL Interception*. Das ist nicht sehr vertrauenswürdig, wenn man sich gegen staatliche Überwachung schützen will.

  Mit DANE/TLSA gibt es einen Ansatz, die SSL-Zertifikate auf einem kryptografisch gesicherten, unabhängigen Weg zu verifizieren. Leider verbreitet es sich nur langsam und wird von den meisten Programmen (noch?) nicht unterstützt.

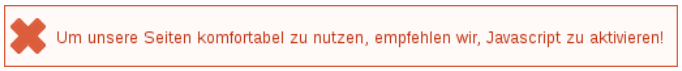
Kapitel 4

Spurenarm Surfen

Das auf den folgenden Seiten vorgestellte Konzept zum spurenarmen Surfen umfasst folgende Punkte:

1. Die Nutzung datensammelnder Webangebote kann man vermeiden.
2. Die Annahme von Cookies und die Ausführung von JavaScript wird auf vertrauenswürdige Webseiten eingeschränkt.
3. Werbung, HTML-Wanzen und die Like-Buttons (mit denen Social Networks wie Facebook Daten sammeln) werden durch Filter blockiert.
4. Verräterische Informationen des Browsers werden manipuliert oder beseitigt, um Fingerprintingd es Browsers zu erschweren.
5. Risikoreiche und Privacy-unfreundliche Features wie Plug-ins für Flash und PDF-Reader, Geolocation-API, Informationen über die Hardware und Performance, WebRTC... werden im Browser deaktiviert.
6. Die Sicherheit von HTTPS-Verbindungen wird durch zusätzliche Überprüfungen und Anzeigen verbessert. Unsichere Cipher werden deaktiviert, um vertrauenswürdige Verschlüsselung nach dem Stand der zivilen Forschung sicherzustellen.

Mit diesen Maßnahmen kann es vorkommen, dass Websites nicht wie erwartet funktionieren. Gute Webdesigner verzichteten auf suspekte Technologien, JavaScript wird sinnvoll eingesetzt und der Surfer auf fehlende Freigaben hingewiesen. Cookies sind meist für Logins nötig und Javascript ermöglicht hübsche Animationen oder Prüfung von Eingaben.



Weniger gute Webseiten liefern seltsame Fehlermeldungen:

Ganz schlechte Websites machen irgendwas, aber nicht was man erwartet. Gelegentlich werden auch Referer oder User-Agent ausgewertet, obwohl es belanglos sein sollte, und Surfer werden nicht auf die notwendigen Freigaben hingeweisen. Hier ist man auf Probieren und Raten angewiesen. Als erstes kann man Cookies freigeben. Wenn das nicht hilft, kann man Javascript gezielt für einzelne Server freigeben oder unsichere SSL Verschlüsselung zulassen. Ob die Deaktivierung der Schutzmaßnahmen die volle Funktionalität aufwiegt, muss man bei Bedarf selbst entscheiden.

4.1 Auswahl des Webbrowsers

Firefox ist der Webbrowser der Mozilla Foundation. Er ist kostenfrei nutzbar und steht auf der Website des Projektes [1] für Windows, MacOS und Linux zum Download bereit. Die *Extented Support Releases*[2] (ESR-Versionen) von Firefox werden im Gegensatz zu den 6-wöchigen Updates des Firefox für ca. ein Jahr gepflegt. Es werden keine neuen Features eingebaut, was sich positiv auf die Stabilität auswirkt. Allerdings fehlen damit auch aktuelle Verbesserungen in der SSL/TLS Verschlüsselung u.ä. Updates, die positiv für die Sicherheit sind.

Linux-Distributionen enthalten den Browser in der Regel. Man kann den Browser mit der Paketverwaltung installieren, für Ubuntu z.B. mit:

```
> sudo apt install firefox firefox-locale-de
```

Debian GNU/Linux enthält den Firefox-ESR. Der Browser wird aus den Repositories mit folgendem Kommando installiert:

```
> sudo apt install firefox-esr firefox-esr-l10n-de
```

apparmor ist ein Sicherheitsframework für Linux. Als Mandatory Access Control System kontrolliert es einzelne Anwendungen und kann mit Profilen die Rechte von Anwendungen fein granular einschränken. Sollte eine Anwendung (z.B. Firefox) kompromittiert werden, kann der Angreifer nur wenig Schaden anrichten, wenn die Anwendung unter Kontrolle von *apparmor* läuft.

Einige Distributionen wie z.B Ubuntu bringen ein apparmor-Profil für Firefox mit. Die Pakete *apparmor-profiles* und *apparmor-utils* sind zu installieren und die Regeln für Firefox zu enforcen:

```
> sudo apt install apparmor-profiles apparmor-utils
> sudo aa-enforce usr.bin.firefox
```

Mit dem Kommando *aa-status* kann man prüfen, ob Firefox im enforced mode unter Kontrolle von *apparmor* läuft, nachdem der Browser gestartet wurde.

Freunde von *BSD finden Firefox im pkgsrc und können die aktuelle Version selbst compilieren.

[1] hhttps://www.mozilla.org/en-US/firefox/all/
[2] https://www.mozilla.org/en-US/firefox/organizations/all.html

Schnellkonfiguration für einen privacy-freundlichen Firefox

Wer sich nicht mit den Details beschäftigen möchte, kann diese Anleitung zur Schnellkonfiguration nutzen, um Firefox privacy-freundlich zu konfigurieren. Das Kapitel *Spurenarm Surfen* mit denn ausführlichen Erläuterungen kann man überspringen und im nächsten Kapitel weiterlesen.

Folgende Add-ons bzw. Konfigurationsdateien empfehlen wir:

- Das Add-on **CookieController** vereinfacht die Website-spezifischen Einstellungen für Cookies und DOMStorage (Super-Cookies) sowie den Zugriff auf gespeicherte Cookies.

- Mit dem Add-on **NoScript** kann man die Einstellungen für Javascript verwalten. Außerdem rüstet es wesentliche Sicherheitsfeatures nach. Bitte lesen Sie die Hinweise für die Konfiguration von NoScript.

- **uBlock Origin** ist ein effizienter und einfach installierberer Werbe- und Trackingblocker für Firefox. Die verwendeten Blocklisten sind konfigurierbar.

- Das Add-on **CanvasBlocker** blockiert das Auslesen von HTML5 Canvas Elementen, um Fingerprinting des Browsers zu verhindern.

- Das Add-on **No Resource URI Leak** blockiert den Zugriff auf *recource://* und *chrome://* Adressen für Websites und verhindert damit das Auslesen von Informationen für das Fingerprinting des Browsers.

- Das Add-on **HTTPSEverywhere** erzwingtt die SSL-Verschlüsselung bei einige Tausend Webseiten und kann das SSL-Obervatory der EFF.org nutzen, um SSL-Zertifikate zusätzlich zu verifizieren.

- Der **DNSSEC/TLSA-Validator** überprüft die SSL-Zertifikate einer Webseite anhand der Fingerprints im DANE/TLSA-Record in DNS. Nach der Installation des Add-on sollte man unbedingt in der Add-on Verwaltung die Einstellungen aufrufen und die DNS-Server Einstellungen testen.

- Außerdem kann man die Datei *user.js* von unserer Webseite https://www.privacy-handbuch.de/handbuch_21u.htm herunter laden und im Firefox Profil speichern. Diese Datei einhält alle auf den folgenden Seiten empfohlenen Werte. Sie wird beim Start von Firefox eingelesen und überschreibt die Default Einstellungen und die Einstellungen in der Datei *prefs.js*.

Um die Installation von privacy-freundliche Suchmaschinen zu vereinfachen, haben wir einige Such-Plugins vorbereitet. Wenn man auf die Webseite https://www.privacy-handbuch.de/handbuch_21browser.htm aufruft, kann man im Suchfeld oben rechts in der Firefox Toolbar ein paar Buchstaben tippen und in dem ausklappenden Menü die gewünschten Suchmaschinen mit einem Klick hinzufügen.

4.2 Datensparsame Suchmaschinen

Suchmaschinen werden sicher am häufigsten genutzt, um sich im Web zu orientieren. Neben den bekannten Datensammlern wie Google, MSN oder Yahoo gibt es durchaus Alternativen.

Für alle alternativen Suchmaschinen gilt, dass sie eine andere Sicht auf das Web bieten und die Ergebnisse sich von Google unterscheiden. Man sollte bei der Beurteilung der Ergebnisse beachten, dass auch Google nicht die reine Wahrheit bieten kann, sondern nur eine bestimmte Sicht auf das Web.

Suchmaschinen mit eigenem Index

Es ist nicht einfach, eine Suchmaschine zu finden, die die Privatsphäre der Nutzer respektiert, einen umfangreichen Index zur Verfügung stellt und gute Ergebnisse liefert. Ein paar Vorschläge:

- **DuckDuckGo.com** (https://duckduckgo.com)
  DuckDuckGo ist eine privacyfreundliche Suchmaschine. Es gibt eine Javascript-freie Version (HTML), aber die Ergebnisse der Javascript Version sind irgendwie besser. Neben der eigentlichen Suche bietet DuckDuckGo viele nette Erweiterungen. Das Suchfeld kann als Taschenrechner genutzt werden oder zum Umrechnen von Einheiten, Fragen nach dem Wetter können beantwortet werden (in englisch: *weather* oder *is it raining*)... u.v.a.m. Eine Übersicht bieten die Goodies und Tech Goodies.[3]

- **Qwant** (https://www.qwant.com)
  Qwant definiert sich selbst nicht als Suchmaschine sondern als Entdeckungsmaschine. Es gibt wie bei DuckDuckGo eine Javascript-freie Lite Version, aber die Suchergebnisse sind mit Freigabe von Javascript und Cookies deutlich besser. Die Bildersuche von Qwant gefällt mir, funktioniert mit sicheren SSL-Einstellungen.

- **Open Directory** (http://www.dmoz.de oder http://www.dmoz.org)
  Das Open Directory ist ein Katalog, der von Freiwilligen gepflegt wird. Man kann die Suche auf Kategorien eingrenzen und erhält übersichtliche Ergebnislisten.

Meta-Suchmaschinen

Meta-Suchmaschinen leiten die Suchanfrage an mehrere Suchdienste weiter. Sie sammeln die Ergebnisse ein und sortieren sie neu.

- **Ixquick.eu/deu** (https://www.ixquick.eu/deu)
  bietet die alte Meta-Suche, mit der die niederländischen Suchmaschine einst gestartet ist. Die Suchmaschine speichert keine IP-Adressen und generiert keine Profile der Nutzer. Ixquick.eu nutzt für allgm. Fragen Yahoo! und Yandex aber nicht Google. Außerdem werden noch einige Spezialsuchemaschinen einbezogen.

[3] https://duckduckgo.com/goodies.html

Als kleines Schmankerl bietet Ixquick die Möglichkeit, aus den Suchergebnissen heraus die Webseiten über einen anonymisierenden Proxy aufzurufen. Die aufgerufene Webseite sieht damit nur eine IP-Adresse von Ixquick. Neben den Ergebnissen findet man einen kleinen Link *Proxy*:

Webinterface of "**awxcnx**" ★★★★
HTTPS: https://www.**awxcnx**.de. MD5-Digest: 52:4A:8C:97:9D:C0:84:3D:12:63:08:
https://www.**awxcnx**.de/ - Proxy - Markieren - 1 weiteres Top-Ergebnis von dieser Site

Aus Sicherheitsgründen entfernt der Proxy Javascript Code aus den aufgerufenen Webseiten. Es ist daher möglich, dass einige Webseiten nicht wie erwartet funktionieren. Außerdem ist KEINE Eingabe von Daten in Textfeldern der aufgerufenen Webseite möglich. Der Proxy kann die Webseiten nur darstellen.

- **Ixquick.com** liefert die Suchergebnisse von Startpage.

- **Startpage** (https://startpage.com)
  wird ebenfalls von Surfboard Holding B.V. betrieben und ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Die Suchmaschine bietet privacy-freundlichen Zugriff auf die Google-Suche, ist also eine Ergänzung zu Ixquick.eu. Den Proxy zum anonymen Aufruf der Webseiten aus den Ergebnissen kann auch nutzen.

Bei Ixquick.com und Startpage ist standardmäßig ein Family-Filter aktiv. Wer etwas Anstößiges sucht, erhält keinen Hinweis auf den Filter sondern nur die Antwort:

> *Es wurden keine mit Ihrer Suchanfrage übereinstimmenden Dokumente gefunden.*

Das Mycroft Project bietet ein Such-Plugin mit ungefilterten Suchergebnissen, das auch Ergebnisse für die Suche nach *Dildos* anzeigt. In den Einstellungen kann man den Filter auch deaktivieren.

- **Disconnect.me** (https://search.disconnect.me/)
  bietet einen privacy-freundlichen Such-Proxy für Google, Yahoo und Bing.

- **Metager.de** (https://www.metager.de/)
  ist ein deutscher Klassiker vom Suma e.V. Neben klassischen Suchdiensten wird auch die Peer-2-Peer Suche Yacy einbezogen. Dadurch verzögert sich die Anzeige der Ergebnisse etwas. Mit Javascript sieht die Seite etwas besser aus, funktioniert aber auch ohne Javascript. Metager.de kann auch als Tor Hidden Service unter folgender Adresse genutzt werden: http://b7cxf4dkdsko6ah2.onion/tor/

Metager bietet wie Ixquick und Startpage einen Proxy, um Ergebnisse aus der Suchliste anonym aufzurufen. Die Server stehen in Deutschland.

Privacy-Handbuch
https://privacy-handbuch.de/ anonym öffnen
Privacy-Handbuch. Wir sind die Vielen.Einleitung Privacy-Levels Nachdenken Spurenarm Surfen Bezahlen im Netz E-Mails (allgm.)
gefunden von: yandex.com

- **UnBubble.eu** (https://unbubble.eu)
  ist eine weitere europäische Metasuchmaschine. Im Gegensatz zu Startpage.com werden die Suchanfragen nicht an Google weitergereicht und keine Google Ergebnisse angezeigt. Der Name ist eine Anspielung auf die FilterBubble, in der wir gefangen sind, wenn wir nur personalisierte Suchergebnisse angezeigt bekommen.

Spezielle Anwendungsfälle

- Wikipedia kann man auch ohne Umweg über Google direkt fragen, wenn man Informationen sucht, die in einer Enzyklopädie zu finden sind.
- Statt Google übersetzen zu lassen, kann man LEO nutzen. Der Translator kennt neben Englisch und Deutsch weitere Sprachen.

Peer-2-Peer Suchmaschine

Yacy [4] ist eine zensurresistente Peer-2-Peer Suchmaschine. Jeder kann sich am Aufbau des Index beteiligen und die Software auf seinem Rechner installieren. Der Crawler ist in Java geschrieben, benötigt also eine Java-Runtime (JRE), die es für WINDOWS bei Oracle [5] zum kostenlosen Download gibt. Linuxer können das Paket *default-jre* mit der Softwareverwaltung installieren. Danach holt man sich die Yacy-Software von der Website des Projektes und startet den Installer - fertig. Für Debian, Ubuntu und Linux Mint bietet das Projekt ein Repository [6] mit fertigen Paketen.

Nach dem Start von Yacy kann man im sich öffnenden Bowserfenster die Basiskonfiguration anpassen und los gehts. Die Suchseite ist im Browser unter http://localhost:8090 erreichbar.

Die Beantwortung der Suchanfragen dauert mit 5-10sec ungewohnt lange. Außerdem muss Javascript für *http://localhost* freigegeben werden, damit die Ergebisseite sauber dargestellt wird. Mit den Topwords unter den Ergebnissen bietet Yacy ein Konzept, um die Suchanfrage zu präzisieren.

Google ???

Anfang Februar 2012 hat Google seine Suchmaschine überarbeitet. Die Webseite macht jetzt intensiven Gebrauch von Javascript. Eine vollständige Analyse der verwendeten Schnüffeltechniken liegt noch nicht vor. Einige vorläufige Ergebnisse sollen kurz vorgestellt werden:

[4] http://yacy.net
[5] http://java.sun.com
[6] http://www.yacy-websuche.de/wiki/index.php/De:DebianInstall

Einsatz von EverCookies: Der Surfer wird mit EverCookie Techniken markiert. Die Markierung wird im DOMStorage gespeichert. Der DOMStorage wurde vom W3C spezifiziert, um Web-Applikationen die lokale Speicherung größerer Datenmengen zu ermöglichen und damit neue Features zu erschließen. Google wertet die User-Agent Kennung und weitere Informationen über den Browser aus, um die Möglichkeit der Nutzung des DOMStorage erst einmal zu prüfen und gegebenenfalls Alternativen wie normale Cookies zu verwenden.

Tracking der Klicks auf Suchergebnisse: Bei Klick auf einen Link in den Suchergebnissen wird die Ziel-URL umgeschrieben. Aus der für den Surfer sichtbaren Zieladresse

```
https://www.awxcnx.de/handbuch.htm
```

wird im Moment des Klick eine Google-URL:

```
http://www.google.de/url?q=https://www.awxcnx.de/......
```

Die zwischengeschaltete Seite enthält eine 302-Weiterleitung auf die ursprüngliche Ziel-URL. Der Surfer wird also fast unbemerkt über einen Google-Server geleitet, wo der Klick registriert wird. Bei deaktiviertem Javascript ist stets die Google-URL sichtbar, nicht die Zieladresse.

Diese Umschreibung der Links gibt es auch bei Bing, Facebook, Youtube und anderen Datensammlern. Das Firefox Add-on Google Privacy kann diese Umschreibung verhindern. Das Add-on ist noch im Beta Status. Die Entwicklung von *Google Privacy* ist ein Wettlauf zwischen Hase und Igel. Einfacher und sicherer ist es, privacy freundliche Suchmaschinen zu nutzen.

Browser Fingerprinting: Mittels Javascript wird die innere Größe des Browserfensters ermittelt. Folgenden Code findet man in den Scripten:

```
I[cb].oc= function() {
var a=0, b=0;
self.innerHeight?(a=self.innerWidth,b=self.innerHeight):....;
return {width:a, height:b}
};
```

Die ermittelten Werte werden als Parameter *biw* und *bih* in der Google-URL übergeben. Sie haben aber keinen Einfluss auf die Bildschirmdarstellung. Auch wenn das Browserfenster zu klein ist und die Darstellung nicht passt, bleibt die Größe der HTML-Elemente erhalten.

Die inneren Abmessungen des Browserfensters sind ein sehr individuelle Parameter, der von Betriebssystem und gewählten Desktop-Einstellungen abhängig sind. Sie werden von der Schriftgröße in der Menüleiste, der Fensterdekoration, den aktivierten Toolbars der Desktops bzw. der Browser usw. beeinflusst. Sie sind für die Berechnung

eines individuellen Fingerprint des Browsers gut geeigent. Anhand des Browser-Fingerprint können Surfer auch ohne Cookies oder EverCookies wiedererkannt werden. Die Google Technik kann dabei besser differenzieren als das Projekt Panopticlick der EFF, das bereits 80% der Surfer eindeutig identifizieren konnte.

Auf der Webseite der Google-Suche kann man dem Tracking kaum entgehen. Wer unbedingt die Ergebnisse von Google braucht, kann die Suchmaschine *Startpage.com* als anonymisierenden Proxy nutzen. Sie ist mit dem Datenschutzsiegel EuroPriSe zertifiziert. Andere Suchmaschinen bieten eine andere Sicht auf das Netz - auch nicht schlecht, erfordert aber etwas Umgewöhnung.

Firefox konfigurieren

Die Suchmaschinen kann man in Firefox in den *Einstellungen* in der Sektion *Suche* konfigurieren.

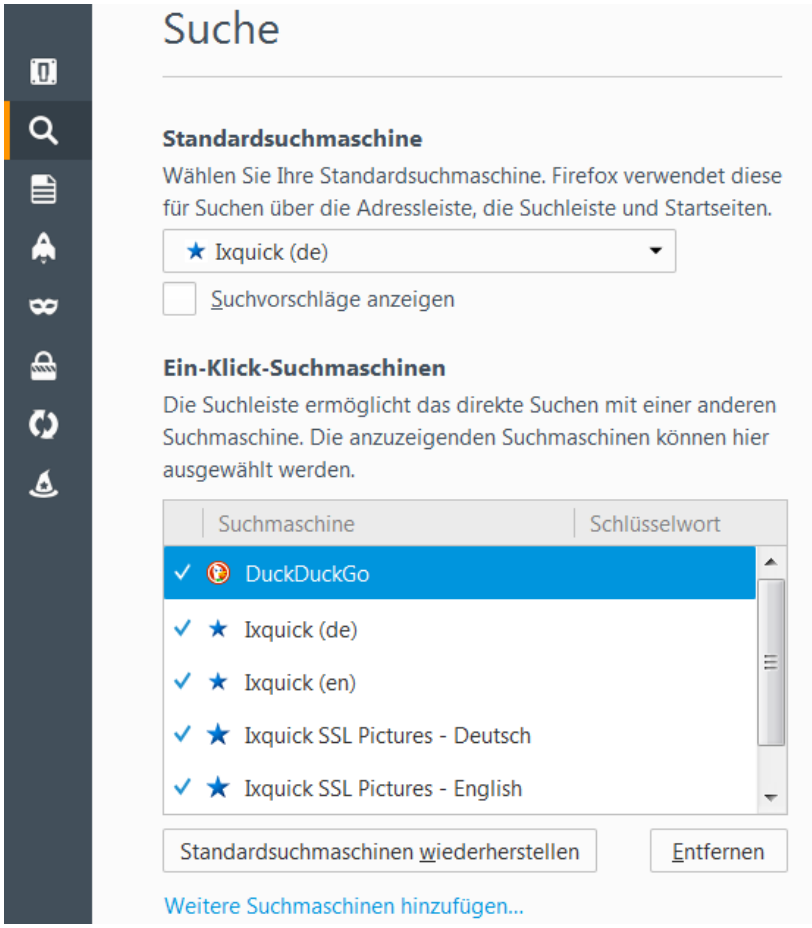


Abbildung 4.1: Suchmaschinen verwalten

Die standardmäßig im Firefox installierten Suchmaschinen verraten überflüssige Informationen über die Installation. Wenn man z.B. unter Ubuntu den Firefox aus dem Repository nutzt, wird bei jeder Suchanfrage irgendwie ein Hinweis auf Ubuntu angehängt:

```
https://www.google.de/search?...&client=ubuntu

https://duckduckgo.com/?...&t=canonical

http://www.amazon.com/s?...&tag=wwwcanoniccom-20
```

Nimmt man den offiziellen Firefox für Windows von der Mozilla Downloadseite, dann werden folgende Informationen angehängt:

```
https://www.google.de/search?...&rls=org.mozilla:de:official

http://www.amazon.com/s?...&tag=firefox-de-21
```

Diese Parameter in der Suchanfrage können einen User-Agent Fake entlarven. Die standardmäßig installierten Suchmaschinen sollte man deaktivieren und statt dessen privacy-freundlichere Plug-ins von mycroft.mozdev.org installieren.[7] zu installieren. In einem Suchformular auf der Webseite gibt man den Namen der Suchmaschine ein und findet schnell ein umfangreiche Liste von Varianten. Für viele Suchmaschinen wie DuckDuckGo, Ixquick, Google, Wikipeadia, Startpage u.a.m. gibt es eine lokalisierte Variante (DE) mit SSL-Verschlüsselung und evtl. ohne Javascript. Diese Variante sollte bevorzugt werden. Ein Klick in der Liste der Ergebnisse installiert das Plug-in. Die Webseite funktioniert nur mit JavaScript.

Die Standardsuchmaschine wird an mehreren Stellen von Firefox ohne weitere Nachfrage genutzt. Es sollte eine privacy-freundliche Suche ausgewählt werden.

Die Generierung von Suchvorschlägen kann man deaktivieren. Die Vorschläge kommen von dem gewählten Standardsuchmaschine, sobald man mit dem Eingabe im Suchfeld beginnt. Es verlangsamt aber die Reaktion auf Eingaben deutlich.

GeoIP-spezifische Standardsuchmaschine deaktivieren

Aus kommerziellen Gründen verwendet Firefox die Suche von Yahoo! als Standardsuchmaschine für US-amerikanische Nutzer. Um den eigenen Standort und damit das Land zu bestimmen, kontaktiert Firefox bei jedem Start den Server *location.services.mozilla.com*. Damit wird die externe IP-Adresse ermittelt und via Geolocation der aktuelle Standort bestimmt.

Um diese überflüssige Verbindungsaufnahme zu unterbinden, kann man unter der Adresse *about:config* folgende Variablen setzen:

```
browser.search.countryCode          = DE
browser.search.geoSpecificDefaults = false
browser.search.geoip.url            = ""    (leerer String)
```

[7] http://mycroft.mozdev.org/

4.3 Cookies

Cookies werden für die Identifizierung des Surfers genutzt. Neben der erwünschten Identifizierung um personalisierte Inhalte zu nutzen, beispielsweise einen Web-Mail-Account oder um Einkäufe abzuwickeln, werden sie überwiegend für das Tracking von Surfern verwendet.

Der Screenshot Bild 4.2 zeigt die Liste der Cookies, die bei einem einmaligen Aufruf der Seite *www.spiegel.de* gesetzt wurden. Es ist nicht ungewöhnlich, dass populäre Webseiten mehrere Datensammler einbinden. Eine Studie der Universität Berkeley [8] hat 2011 beim Surfen auf den TOP100 Webseiten 5.675 Cookies gefunden (ohne Login oder Bestellung). 4.914 Cookies wurden von Dritten gesetzt, also nicht von der aufgerufenen Webseite. Die Daten wurden an mehr als 600 Server übermittelt. Spitzenreiter unter den Datensammlern ist Google. 97% der populären Webseiten setzen Google-Cookies.

Immer mehr Tracking Dienste gehen dazu über, die Cookies im First-Party Context zu setzen, da Cookies von Drittseiten recht einfach blockiert werden können. Eine empirische Studie der Universität Leuven von 2014 zeigt, dass 44 verschiedene Tracking Dienste mehr als 40% des Surfverhaltens mit Hilfe von Cookies verfolgen können, auch wenn man Cookies für Drittseiten blockiert und nur First-Party Cookies erlaubt. Die Cookies werden mit Javascript geschrieben oder der Tracking Dienst erschleicht sich mit einem DNS-Alias als Subdomain der besuchten Webseite First-Party Status.[9]

Die Tracking-Cookies werden auch von der NSA und GCHQ im Rahmen der globalen Überwachung genutzt. Die Geheimdienste beobachten den Datenstrom im Internet und identifizieren Surfern anhand langlebiger Cookies, insbesondere das Google PREF Cookie wird von den Überwachern gern genutzt. Zielpersonen werden anhand dieser Cookies verfolgt und bei Bedarf mit *Foxit Acid* gezielt angegriffen, wenn die Identifikation für mindestens 2 Wochen stabil möglich ist.[10]

Sinnvoll ist ein **Whitelisting** für die Behandlung von Cookies:

1. Standardmäßig wird die Annahme von Cookies verweigert.
2. Für vertrauenswürdige Websites, welche die Nutzung von Cookies zur vollen Funktion benötigen, werden Ausnahmen zugelassen.
3. Alle gespeicherten Cookies werden beim Schließen des Browsers automatisch gelöscht.

Fast alle Login-Seiten, welche Cookies zur Identifizierung des Surfers verwenden, weisen mit einem kleinen Satz auf die notwendigen Freigaben hin. Treten beim Login seltsame Fehler auf, z.B. ständig die Fehlermeldung *FALSCHES PASSWORT*, verweigert der Browser wahrscheinlich die Annahme von Cookies. Die Website sollte in die Liste der vertrauenswürdigen Websites

[8] http://heise.de/-1288914
[9] https://securehomes.esat.kuleuven.be/ gacar/persistent/the_web_never_forgets.pdf
[10] https://www.eff.org/deeplinks/2013/12/nsa-turns-cookies-and-more-surveillance-beacons

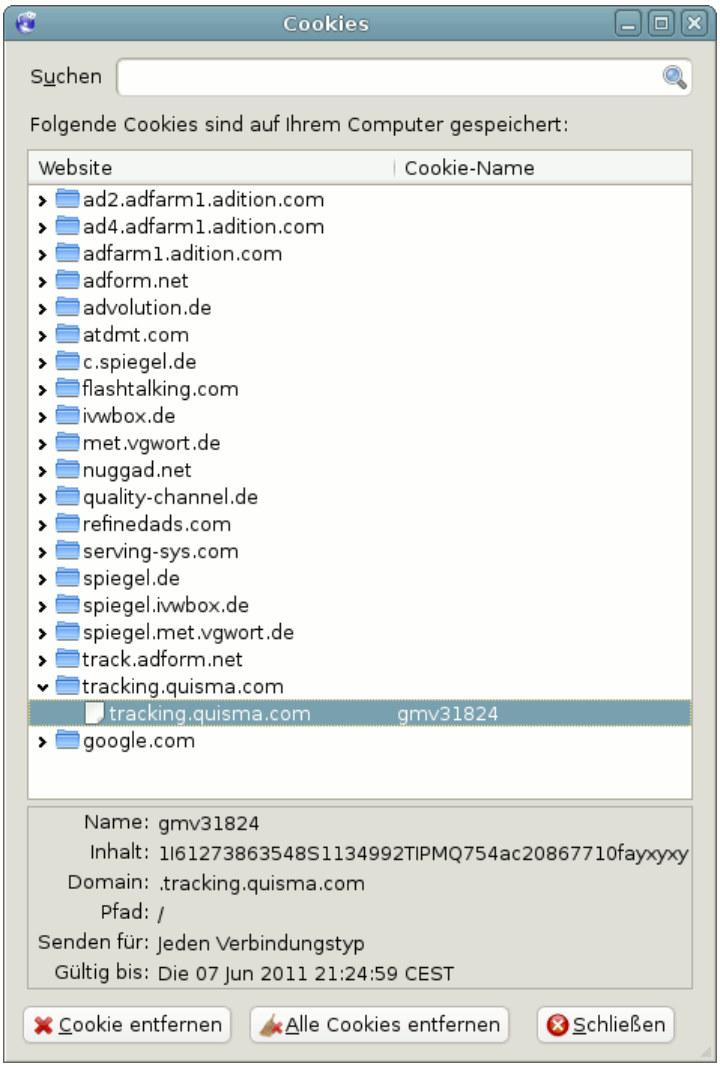


Abbildung 4.2: Liste der Cookies beim Besuch von Spiegel-Online

aufgenommen werden oder man muss Cookies temporär erlauben.

Mozilla Firefox konfigurieren

Mozilla Firefox bietet bereits standardmäßig die Möglichkeit, die meisten Cookies ohne Einbußen am Surf-Erlebnis loszuwerden. Im Bild 4.3 gezeigte Dialog *Einstellungen* Sektion *Datenschutz* kann die Annahme von Cookies standardmäßig deaktiviert werden.

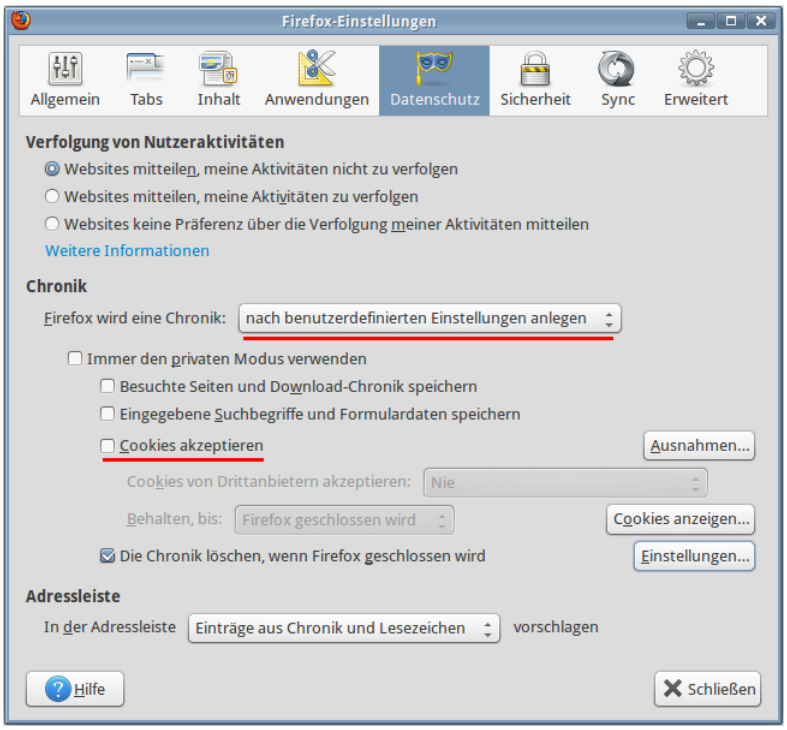


Abbildung 4.3: Cookies-Einstellungen in Firefox

Mit einem Klick auf den Button *Ausnahmen* kann man Webseiten konfigurieren, die Cookies setzen dürfen. In der Regel sind das alle Webseiten, die einen Login erfordern.

Außerdem sollte man die Option *Chronik löschen, wenn Firefox geschlossen wird* aktivieren und in den Einstellungen für diese Funktion das Löschen der Cookies aktivieren.

Das Add-on **Cookie Controller** [11] ist empfehlenswert. Es erlaubt die site-spezifische Verwaltung von Cookies. Ein einfacher Klick auf das Install-Symbol der Website startet den Download der Erweiterung und installiert sie.

[11] https://addons.mozilla.org/en-US/firefox/addon/cookie-controller/

DOMStorage in Firefox

Mozilla Firefox bietet auch die clientseitige HTML5 Datenspeicherung. Dieser DOMStorage oder Web-Storage wird gelegentlich auch als Super-Cookie bezeichnet, da bis zu 5 MB große Datenmengen mit Hilfe von Javascript abgelegt werden können.

Aktuelle Versionen von Firefox wenden die Beschränkungen für Cookies auch auf den DOMStorage an. Es reicht aus, die Cookies zu deaktivieren. Damit ist auch die clientseitige Datenspeicherung deaktiviert. Der DOMStorage wird auch zusammen mit den Cookies gelöscht. Diese parallele Anwendung der Einstellung für Cookies auf DOMStorage gilt nur für Firefox. Andere Browser verhalten sich bezüglich der clientseitigen Datenspeicherung anders!

Indexed Database API

Am 08.01.2015 hat das W3C die *Indexed Database API* als Standard verabschiedet. Dabei handelt es sich um eine hierarchische Datenbank im Browser, die mit Javascript genutzt werden kann. Im Unterschied zum DOM-Storage können nicht nur Key-Value-Paare gespeichert werden, sondern mittels SQL auch komplexe Abfragen realisiert werden.

Wie jede Technologie, die Daten im Browser speichert, kann die Indexed Database ähnlich wie Cookies für die Markierung von Surfern für Trackingzwecke genutzt werden. Forscher der KU Leuven (Belgien) haben darauf hingewiesen, das diese Technik bereits genutzt wird und näher untersucht werden sollte.

Um die Indexed Database API im Firefox abzuschalten, ist unter *about:config* folgender Wert zu setzen:

```
dom.indexedDB.enabled = false
```

Flash-Cookies

Aus Sicherheitsgründen empfehle ich, keinen Flash Player zu nutzen. Wenn man auf Flash absolut nicht verzichten kann, dann findet man die privacyfreundliche Konfiguration des Adobe Flash-Players in einem gesonderten Abschnitt für Plug-ins.

4.4 EverCookies

80% der Internetnutzer lehnen das Tracking ihres Surfverhaltens ab. Viele Surfer ergreifen einfache Maßnahmen gegen Tracking Cookies. Nach einer Untersuchung von AdTiger blockieren 52,5% der Surfer die Annahme von Cookies, die nicht von der aufgerufenen Website stammen (sogenannte Third-Party-Cookies). Andere Studien [12] kommen auf 15%...35% Cookie-Verweigerer

[12] http://smorgasbork.com/component/content/article/84-a-study-of-internet-users-cookie-and-javascript-settings

unter den Surfern (was mir seriöser erscheint). Dabei handelt es meist um Surfer, die regelmäßig auf dem Datenhighway unterwegs sind und somit die Erstellung präziser Profile ermöglichen könnten. Von Gelegenheits-Surfern kann man kaum umfassenden Interessen-Profile erstellen.

Die Tracking-Branche reagiert auf diese Entwicklung mit erweiterten Markierungen, die unter der Bezeichnung *EverCookie* zusammengefasst werden. Zusätzlich zum Tracking-Cookie werden weitere Markierungen im Browser gespeichert. Später kann ein gelöschtes Tracking-Cookie anhand dieser Markierungen wiederhergestellt werden.

Nach empirischen Untersuchungen der University of California [13] nutzen viele Trackingdienste EverCookie Techniken. Häufig werden seit 2005 Flash-Cookies bzw. LSOs parallel zu normalen Cookies eingesetzt, wobei diese Technik auf dem absteigenden Ast ist. 2011 nutzen 37% der TOP100 Webseiten diese Technik, 2012 nur noch 17%. Die Flash-Cookies werden durch HTML5-Techniken wie DOMstorage und ETags ersetzt. 31% der TOP100 Webseiten nutzen moderne HTML5-Techniken zur Markierung der Surfer (Stand 2012).

- Die *Google-Suche* nutzt DOMstorage, was eine Markierung von Nutzern auch bei deaktivierten Cookies ermöglichen soll.
- Die Firma *Clearspring* protzt damit, präzise Daten von 250 Mio. Internetnutzern zu haben. Sie setzte bis 2010 Flash-Cookies ein, um gelöschte Cookies wiederherzustellen.
- *Ebay.de* verwendet Flash-Cookies, um den Browser zu markieren.
- *AdTiger.de* bietet umfangreiche Angebote zur gezielten Ansprache von Surfern und protzt damit, 98% der Zugriffe über einen Zeitraum von deutlich länger als 24h eindeutig einzelnen Nutzern zuordnen zu können. Nach einer eigenen Studie kann AdTiger aber nur bei 47,5% der Surfer normale Cookies setzen.
- Die Firma *KISSmetrics* (*"a revolutionary person-based analytics platform"*) setzte zusätzlich zu Cookies und Flash-Cookies noch ETags aus dem Cache, DOMStorage und IE-userData ein, um Surfer zu markieren. Aufgrund der negativen Schlagzeilen wird seit Sommer 2011 auf den Einsatz von ETags verzichtet.

EverCookies - never forget

Der polnische Informatiker Samy Kamkar hat eine Demonstration [14] von EverCookie Techniken erstellt, die verschiedene technische Möglichkeiten basierend auf HTML5 zeigen:

- Local Shared Objects (Flash Cookies)
- Silverlight Isolated Storage
- Cookies in RGB Werten von automatisch generierten Bildern speichern

[13] http://www.law.berkeley.edu/privacycensus.htm
[14] http://samy.pl/evercookie/

- Cookies in der History speichern
- Cookies in HTTP ETags speichern
- Cookies in Browser Cache speichern
- window.name auswerten
- Internet Explorer userData Storage
- HTML5 DOMStorage
- HTML5 Database Storage (IndexedDB)
- HTTP-Auth speichern

Verteidigungsstrategien

Zur Verteidigung gibt es drei Möglichkeiten:

1. Die Verbindung zu Tracking-Diensten kann mit **AdBlockern** komplett verhindert werden. Es sind Filterlisten zu nutzen, die in der Regel als Privacy Listen bezeichnet werden.

2. Viele EverCookie Techniken nutzen Javascript. Die Freigabe von Javascript nur auf wenigen, vertrauenswürdigen Seiten schützt ebenfalls. HTML5 DOMStorage folgt den Freigaben für Cookies und Hinweise zur Configuration des Cache zur Vermeidung langfristiger Markierungen mit ETags findet man weiter unter.

3. Die Verwendung von HTML5 IndexedDB zur Wiederherstellung gelöschter Tracking Cookies wurde von Forschern der Universität Leuven (Belgien) erstmals im Sommer 2014 in the wild nachgewiesen. Als Schutz gegen diese EverCookies kann man die IndexedDB in Firefox deaktivieren:

   ```
   dom.indexedDB.enabled = false
   ```

Einen EverCookie-sicherer Browser kann nur mit Konfigurationseinstellungen nicht erreichen. Der Datenverkehr ist durch zusätzliche Maßnahmen zu reinigen. Bisher kann nur der **JonDoFox** und der **JonDoBrowser** alle von Samy Kamkar vorgestellten Techniken während des Surfens blockieren.

Der **TorBrowser** blockiert EverCookies beim Surfen nicht sondern beseitigt alle Markierungen beim Beenden der Surf-Session (Schließen des Browsers oder *Neue Identität* im TorButton wählen). Während der Session ist man anhand von EverCookies wiedererkennbar. Dieses Verhalten entspricht der Zielstellung der Tor-Entwickler.

4.5 JavaScript

JavaScript ist eine der Kerntechniken des modernen Internet, birgt aber auch einige Sicherheitsrisiken.

1. Mit Hilfe von Javascript kann man ein Vielzahl von Informationen über den Browser und das Betriebssystem auslesen. Bildschirmgröße, Farbeinstellungen, installierte Schriftarten... Diese Informationen können zu einem individuellen Fingerabdruck des Browsers verrechnet werden (siehe: Kapitel *Tracking Techniken* in der Einleitung).

2. EverCookie Techniken nutzen Javascript, um zusätzliche Markierungen im Browser zu hinterlegen und gelöschte Tracking Cookies wiederherzustellen.

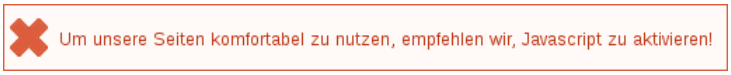
3. Bösartiger Javascript Code kann aktiv Sicherheitslücken im Browser ausnutzen und den Rechner kompromittieren. Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Internet Explorer kompromittierten. Auch die bisher bekannten Exploits von NSA/FBI gegen den TorBrowser nutzten bösartiges Javascript.

4. Forscher der Columbia University haben eine side-channel attack vorgestellt, die komplett als Javascript im Browser läuft: *The Spy in the Sandbox – Practical Cache Attacks in Javascript*[15]. Mit dem Angriff können beliebige Prozesse außerhalb des Browsers analysiert werden ohne den Rechner zu kompromittieren (spurenfrei). Seitenkanalangriffe sind ein moderner Angriff gegen Kryptografie.

5. Bösartiger Javascript Code kann sich auch gegen Dritte richten, ohne das der Nutzer es bemerkt. Chinas Great Cannon[16] injiziert Javascript Code beim Aufruf chinesischer Webseiten, um die PCs der Nutzer als Botnet für DDoS-Attacken zu nutzen.

Prinzip Whitelisting

Ein generelles Abschalten ist heutzutage nicht sinnvoll. Ähnlich dem Cookie-Management benötigt man ein Whitelisting, welches JavaScript für vertrauenswürdige Websites zur Erreichung der vollen Funktionalität erlaubt, im allgemeinen jedoch deaktiviert. Gute Webdesigner weisen den Nutzer darauf hin, dass ohne Javascript eine deutliche Einschränkung der Funktionalität zu erwarten ist.



[15] http://arxiv.org/pdf/1502.07373v2.pdf
[16] https://citizenlab.org/2015/04/chinas-great-cannon/

4.5.1 NoScript für Mozilla Firefox

Die Einstellungen für JavaScript lassen sich mit dem Add-on *NoScript* komfortabel verwalten. Die Erweiterung kann von der Website [17] installiert werden. Ein Klick auf das Install-Symbol der Website installiert die Erweiterung.

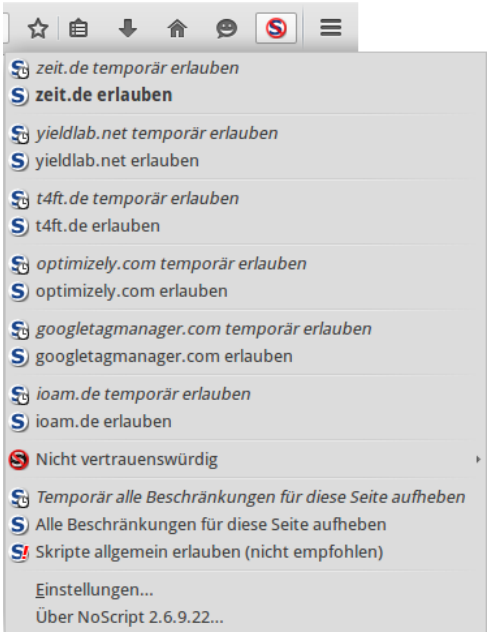


Abbildung 4.4: NoScript-Button und Menü in der Toolbar

Nach dem Neustart von Firefox ist in der Toolbar ein zusätzliches Symbol vorhanden, dass den Status der Freigabe für Javascript anzeigt. Ein Klick auf das Symbol öffnet das im Bild 4.4 gezeigte Menü, welches Javascript für die aktuell relevanten Webseiten generell oder temporär für die Sitzung freigibt.

Skripte von Drittseiten

Skripte von Drittanbietern (googletagmanager, ioam...) werden üblicherweise nur zum Spionieren verwendet und sind für die Funktionalität selten notwendig. Ausnahmen von dieser Regel sind:

Captchas: Einige Webseiten verwenden Captchas von Drittanbietern als Spamschutz. Die Captchas funktionieren nur, wenn Javascript für den Captcha-Provider freigegeben wird. Wenn das Captcha auf einer Webseite nicht funktioniert, kann man in der Liste nachschauen, ob evtl. ein Captcha-Provider dabei ist und diese temporär freigeben.

- Für das häufig verwendete Google Captcha muss man bspw. Javascript temporär für *google.com* und *gstatic.com* freigeben.

[17] https://addons.mozilla.org/de/firefox/addon/noscript

Videos: Firefox braucht keinen Flash Player, um Videos abspielen zu können, aber man muss Javascript für einige Drittseiten freigegeben:

- Um Youtube Videos abspielen zu können, muss man Javascript für *youtube.com*, *ytimg.com* und *googlevideo.com* freigeben. Da viele Webseiten Youtube Videos einbinden, kann man diese Freigaben dauerhaft speichern.
- Um Videos bei Golem.de abspielen zu können, muss man Javascript für *golem.de* und *s3.amazonaws.com* freigeben.
- RT.com bindet Videos von Youtube in die Webseite ein. Zum Abspielen muss man Javascript für *www.rt.com* freigeben und für die Youtube Domains *youtube.com*, *ytimg.com* und *googlevideo.com*.
- Um Videos von Bild.de abzuspielen, muss man Javascript für *bild.de* und *bildstatic.de* temporär freigeben.
- Für Youporn Videos muss man Javascript für die Domainnamen *youporn.com* und *phncdn.com* temporär freigeben.

Wählt man den Punkt *Einstellungen* im NoScript-Menü, öffnet sich der Einstellungsdialog (Bild 4.5), der auf dem Reiter *Positivliste* eine Liste der Websites zeigt, für die Javascript freigegeben wurde. Als Erstes sollte man aus der Positivliste alles entfernen, was man nicht braucht (z.B. google.com). Damit diese Positivliste nicht von NoScript durch Updates modifiziert wird, ist unter *about:config* folgende Variable zu setzen:

```
noscript.allowWhitelistUpdates = false
```

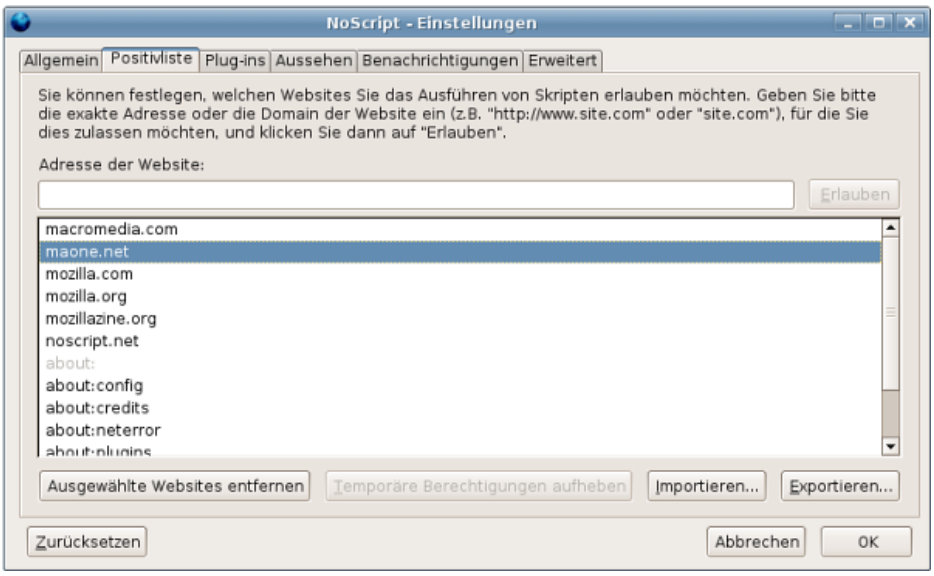


Abbildung 4.5: Einstellungen für NoScript

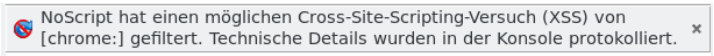
Auf dem Reiter *Benachrichtigungen* lässt sich beispielsweise konfigurieren, ob NoScript den Surfer mit einem Sound oder mit einem Info-Balken darüber

informieren soll, dass Scripte auf der aktuellen Webseite blockiert wurden. Wenn eine Webseite jedoch nicht wie erwartet funktioniert, kann die kurze Einblendung eines Info-Balkens hilfreich sein, sie nervt aber auch.

Sicherheitsfunktionen

NoScript dient nicht nur der Steuerung von Javascript, es bietet **Schutz gegen vielfältige Angriffe** aus dem Netz. (XSS-Angriffe, Webbugs, Click-Hijacking....).

Im Gegensatz zum Internet Explorer und den auf Webkit basierenden Browsern wie Google Chrome hat Firefox keinen eingebauten Schutz gegen XSS-Angriffe. NoScript rüstet diese fehlende Sicherheitsfunktion nach und zeigt eine Warnung bei einem XSS-Angriff:



Die XSS-Protection von NoScript ist standardmäßig aktiv und muss nicht wie beim Internet Explorer oder Google Chrome durch den Webserver mit dem HTTP Response Header *X-XSS-Protection: 1; mode=block* aktiviert werden. Bei Problemen kann man in den Einstellungen von NoScript in einer Whitelist definieren, auf welchen Webseiten die XSS-Protection deaktiviert werden soll.

Application Boundary Enforcer (ABE)

Auf der [TAILS-Dev] Mailingliste wurde darauf hingewiesen, dass ein Angreifer oder Trackingdienst Javascript Code in eine Webseite einbetten könnte, der das interne LAN nach Servern scannt oder versucht lokale Dienste wie den Druckerservice CUPS unter der Adresse http://localhost:631 zu kontaktieren und diese Informationen zum Fingerprinting nutzt, um den Surfer später wiederzuerkennen[18].

Bösartiger Javascript Code könnte lokale Dienste wie CUPS oder andere Rechner im LAN angreifen. Im Mai 2015 wurde ein Exploit-Kit entdeckt, der als bösartiges Javascript auf Webseiten platziert wird und beim Aufruf der Webseite den Router angreift um die DNS Einstellungen zu ändern und damit den Internetzugriff beliebig zu manipulieren[19].

NoScript bietet mit dem *Application Boundary Enforcer* (ABE) einen Schutz gegen diesen Angriff. Unter *Erweitert* auf dem Reiter *ABE* kann man dieses Feature konfigurieren. Die Option *WAN-IP als LOCAL* sollte man deaktivieren, weil NoScript sonst bei jedem Start des Browsers einen externen Server kontaktiert, um die externe IP-Adresse zu ermitteln.

[18] https://mailman.boum.org/pipermail/tails-dev/2015-April/008607.html
[19] http://heise.de/-2665387

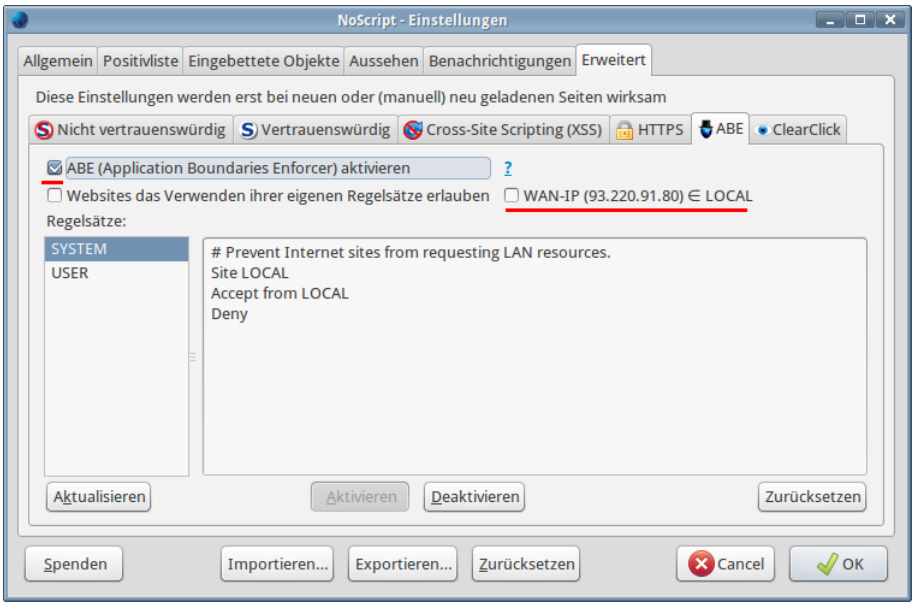


Abbildung 4.6: Einstellungen für NoScript

Javascript Security Einstellungen

Mit kleinen Anpassungen der Einstellungen unter der Adresse *about:config* kann man die Robustheit von Javascript gegen Exploits wie z.B CVE-2015-0817 [20] verbessern. Diese Vorschläge verringern die Performance von Javascript geringfügig aber nicht signifikant:

```
javascript.options.ion            = false
javascript.options.baselinejit    = false
javascript.options.asmjs          = false
```

Die Javascript SharedWorker erlauben den Datenaustausch zwischen den IFrames in Webseiten, die in unterschiedlichen Tabs geöffnet sind, auch wenn die Webseiten nicht zur selben Domain gehören. Dieses Feature sollte deaktiviert werden, da es z.B. Trackingdiensten Synchronisierungen von Daten ermöglicht.

```
dom.serviceWorkers.enabled                = false
dom.serviceWorkers.interception.enabled   = false
```

Außerdem kann man das ganze Push-Geraffel deaktivieren, braucht man nicht, um sich Webseiten anzuschauen:

```
dom.push.enabled              = false
dom.push.connection.enabled   = false
```

[20] https://www.mozilla.org/en-US/security/advisories/mfsa2015-29/

4.6 iFrames

Einige Trackingdienste verwenden iFrames, um HTML-Wanzen zu laden, wenn Javascript blockiert ist und keine Trackingscripte ausgeführt werden können. Auf vielen Webseiten findet man den Code von GoogleTagManager (*Google Universal Analytics tracking code*):

```
<noscript>
  <iframe src="//www.googletagmanager.com/ns.html?id=blabala..."
    height="0" width="0" style="display:none;visibility:hidden">
  </iframe>
</noscript>
```

Die Tracking Technik des *DoubleClick Bid Manager* wurde von Invite Media entwickelt und in DoubleClick integriert, nachdem Google die Firma Invite Media aufgekauft hatte. Auch dieses Tracking nutzt einen unsichtbaren iFrame, um Tracking Wanzen mit oder ohne Javascript zu platzieren:

```
<script type="text/javascript">
...
 <document.write('
    <iframe src="http://nnnn.fls.doubleclick.net/activityi;src=xxxx;...."
    width="1" height="1" frameborder="0" style="display:none"></iframe>');
</script>
<noscript>
  <iframe src=""http://nnnn.fls.doubleclick.net/activityi;src=xxxxx;"
    width="1" height="1" frameborder="0" style="display:none">
  </iframe>
</noscript>
```

Für Webdesigner sind iFrames eine Technik aus dem vergangenen Jahrhundert und werden kaum noch verwendet. Man kann iFrames generell mit NoScript blockieren ohne wesentliche Einschränkungen beim Surfen (Bild 4.7). An Stelle des blockierten iFrames zeigt NoScript einen Platzhalter an. Bei Bedarf kann man den blockierten iFrame mit einem Klick auf das Platzhaltersymbol laden. Vertrauenswürdige Websites dürfen eigene iFrames ohne Bestätigung laden.

4.7 Werbung, HTML-Wanzen und Social Media

Die auf vielen Websites eingeblendete **Werbung** wird von wenigen Servern bereitgestellt. Diese nutzen häufig (eigentlich immer) die damit gegebenen Möglichkeiten, das Surfverhalten über viele Websites hinweg zu erfassen.

Immer häufiger nutzen Kriminelle die große Werbenetzwerke, um mit ihre Schadsoftware möglichst vielen Rechnern anzugreifen. Nach Beobachtung von Trend Micro[21] kaufen Kriminelle zur Zielgruppe passende Werbeplätze, lassen bösartige Werbebanner ausliefern oder locken die Surfer mit Anzeigen auf

[21] http://heise.de/-2429990

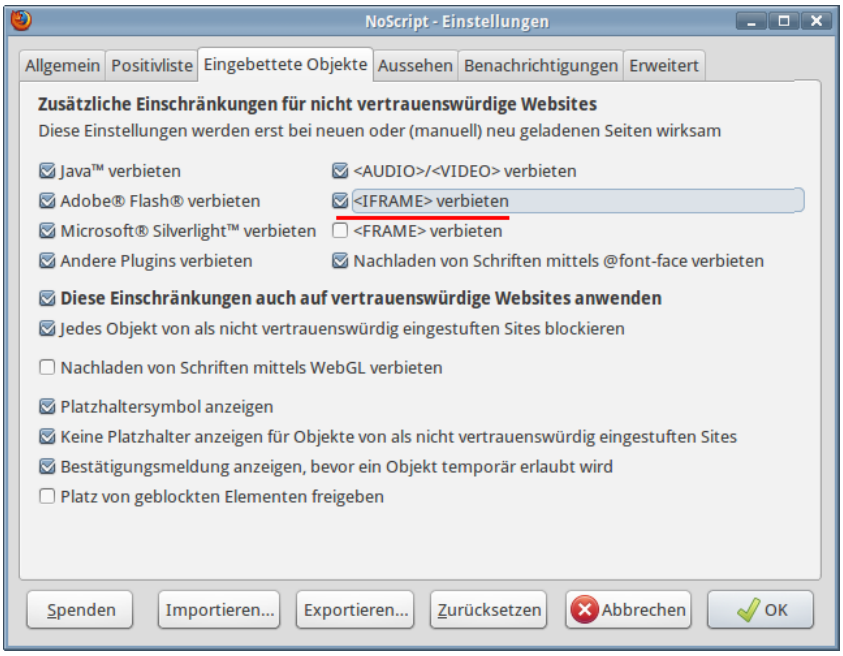


Abbildung 4.7: iFrames mit NoScript blockieren

Malware Webseiten. Diese Angriffe werden als Malvertising bezeichnet (abgeleitet von *malicious advertising*) und nehmen derzeit stark zu. Die Sicherheitexperten von Cyphort registrierten 2015 einen Anstieg von 325% und erwarten eine Fortsetzung dieses Trends für 2016. Einige Beispiele für derartige Angriffe:

- Im Januar 2013 lieferten die Server des Werbenetzwerkes OpenX bösartige Scripte aus, die den Rechner über Sicherheitslücken im Java Plug-in und im Internet Explorer kompromittierten.[22]
- Zum Jahreswechsel 2014 wurden innerhalb von 4 Tagen 27.000 Surfer durch Werbung von Yahoo mit Malware infiziert.[23]
- Eine erfolgreiche, mehrwöchige Malvertising Kampagne konnte im Aug. 2015 mit Hilfe von Doubleclick einige Millionen Surfer infizieren.[24]
- Im Nov. 2015 wurden die Server des Werbenetzwerkes Pagefair gehackt, um bösartigen Javascript Code in der Werbung auszuliefern.[25]

Bei **HTML-Wanzen** (sogenannten Webbugs) handelt es sich um 1x1-Pixel große transparente Bildchen, welche in den HTML-Code einer Webseite oder

[22] http://heise.de/-1787511
[23] http://www.zdnet.de/88180242/werbung-auf-yahoo-com-verteilte-malware-an-nutzer-in-europa
[24] https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/
[25] http://www.golem.de/news/anti-adblocker-dienst-500-websites-ueber-pagefair-gehackt-1511-117262.html

einer E-Mail eingebettet werden. Sie sind für den Nutzer unsichtbar und werden beim Betrachten einer Webseite oder beim Öffnen der E-Mail von einem externen Server geladen und ermöglichen es dem Betreiber des Servers, das Surfverhalten websiteübergreifend zu verfolgen.

Die **Like Buttons** werden von Facebook und anderen Soziale Netzen verwendet, um Daten zu sammeln. Mit dem Aufruf einer Webseite mit Facebook Like Button werden Daten an Facebook übertragen und dort ausgewertet, auch wenn der Surfer selbst kein Mitglied bei Facebook ist. Die Verwendung der Like Buttons ist nach Ansicht von Thilo Weichert (ULD) nicht mit deutschen Datenschutzrecht vereinbar. Deutsche Webseitenbetreiber sind aufgefordert, die Facebook Buttons von ihren Seiten zu entfernen[26].

Forscher der Universität Cambridge (Großbritannien) konnten im Rahmen einer Untersuchung durch Auswertung der Klicks auf Facebook Like Buttons die sexuelle Orientierung und politische Einstellung der Teilnehmer vorhersagen[27]. Man verrät mit einem Klick auf einen Like Button möglicherweise Informationen, die man nicht im Netz veröffentlichen möchte.

4.7.1 Tracking-Filter für Firefox

Es gibt mehrere Add-ons für Firefox, die Werbung und Trackingelemente blockieren. Das Center for Internet and Society der Stanford Law School hat in einer Analyse vom September 2011 einige Lösungen verglichen [28]. Die Ergebnisse in Bild 4.8 zeigen: keine Lösung ist perfekt.

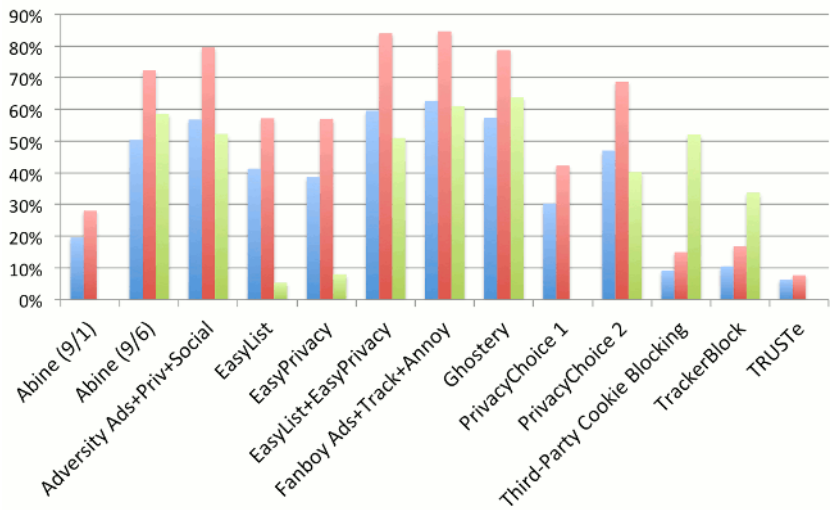


Abbildung 4.8: Effektivität verschiedener Tracking-Filter

[26] https://www.datenschutzzentrum.de/facebook
[27] http://heise.de/-1820638
[28] https://cyberlaw.stanford.edu/node/6730

Aufgrund der Flexibilität bei der Einbindung verschiedener Filterlisten und der langfristigen Stabilität in der Entwicklung sind
textituBlock Origin und textitAdBlock Plus empfehlenswert. Mit den Easylist Filterlisten erreichen die Add-ons die besten Ergebnisse. Die Listen werden ständig weiterentwickelt. Zusätzlich zur den Blocklisten gegen Werbung und Tracking gibt es auch Listen, die die Social Media Buttons blockieren. FanBoy arbeitet seit 2010 mit EasyList zusammen, daher die gleichfalls guten Ergebnisse.

Ghostery schneidet im Test auch gut ab und wird oft empfohlen. Insbesondere in der Diskussion um Acceptable Ads in AdBLock Plus wird Ghostery immer wieder als angeblich saubere Alternative genannt. Dabei wird übersehen, das Ghostery z.B. bei den Trackingdiensten Drawbridge[29] und Tapad[30] als Partner gelistet ist. Die Spezialität dieser Trackingdienste ist die Identifikation der unterschiedlichen Geräte (Smartphones, Computer auf der Arbeit und zuhause, Laptops, Tablets), die von einem User benutzt werden. Die Kooperation mit den Trackingdiensten ist auf der Ghostery Webseite[31] nicht klar beschrieben und nicht offengelegt. Möglicherweise handelt es sich dabei um die via Ghostrank von dem Browser Add-on gesammelten Daten? Da diese Zusammenarbeit mit der Werbeindustrie und die resultierenden Folgen wie *Ghostery Verified Domains* undurchsichtig sind, wird Ghostery hier NICHT empfohlen.

4.7.2 Tracking Protection in Firefox

Am einfachsten kann man ab Firefox 39.0 einen integrierten Trackingschutz unter der Adresse *about:config* aktivieren, indem man folgende Variablen setzt:

```
privacy.trackingprotection.enabled = true
```

Es wird eine Blockliste von Disconnect genutzt, die von einem Mozilla-Server heruntergeladen wird. Diese Blockliste ist nicht dafür ausgelegt, Werbung auf allen Webseiten zu blockieren. Sie blockiert Trackingdienste und damit quasi als Nebeneffekt Werbebanner, die für das Tracking genutzt werden. Ab Firefox 42.0 ist der Trackingschutz standardmäßig im *Private Browsing Mode* aktiviert.

4.7.3 uBlock Origin für Firefox

uBlock Origin[32] ist ein effizienter und einfach installierberer Werbeblocker für Firefox. Zur Installation muss man nur auf den Downloadbutton auf der Webseite klicken.

Nach der Installation findet man oben rechts in der Toolbar des Browsers das uBlock Symbol. Mit einem Klick auf des Symbol kann man die Filterung für die aktuelle Webseite anpassen oder ganz deaktivieren. Neben Werbung

[29] http://drawbrid.ge
[30] http://www.tapad.com
[31] https://www.ghostery.com
[32] https://addons.mozilla.org/de/firefox/addon/ublock-origin

blockiert uBlock Origin auch den Download von Schriftarten. Wenn einzelne Webseiten wegen falscher Symbole unbenutzbar werden, kann man der Webseite den Download von externen Schriften erlauben oder die Webiconfonts lokal installieren, wie es unter *Installierte Schriftarten verstecken* beschrieben ist.

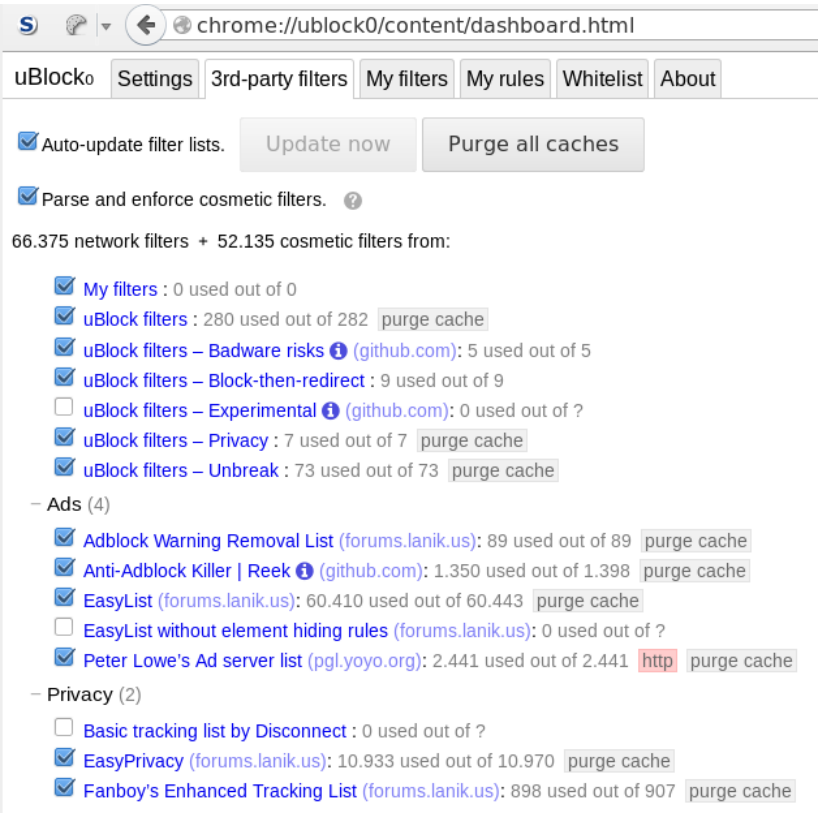


Abbildung 4.9: Dashboard von uBlock Origin

Unter der Adresse *chrome://ublock0/content/dashboard.html* kann man die Konfiguration anpassen und auf dem Reiter *3rd-party filters* weitere Filterlisten aktivieren, z.B. *Fanboy's Social Blocking List* oder *EasyList Germany* sowie die *Anti-AdBlock-Killer* Liste, die wieder das werbefreie Lesen von Bild.de und ähnlichen Webseiten ermöglicht. Aus Sicherheitsgründen würde ich keine Listen abonnieren, die über eine unverschlüsselt HTTP-Verbindung aktualisiert werden (erkennbar an dem roten Symbol *http*).

4.7.4 Adblock Plus für Firefox

Adblock Plus[33] ist ein Klassier für das listenbasierte Blockieren von Werbung. Für AdBlock Plus gibt es viele Listen zum Blockieren von Werbung (länderspezifisch), Tracking-Diensten und der Social Media Like-Buttons. Ein

[33] https://addons.mozilla.org/de/firefox/addon/adblock-plus

einfacher Klick auf das Install-Symbol der Website startet den Download der Erweiterungen und installiert sie.

Nach dem Neustart ist mindestens eine Filterliste zu abonnieren (Bild 4.10). Standardmäßig wird für deutsche Benutzer die Liste *EasyList Germany + EasyList* vorgeschlagen. *EasyList* ist eine gute Wahl, die man akzeptieren kann.

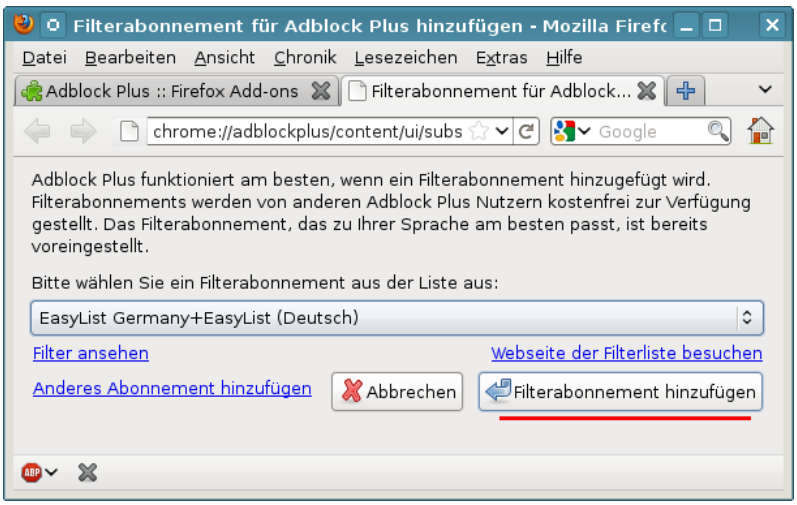


Abbildung 4.10: Auswahl einer Liste nach der Installition von Adblock Plus

Weitere Filterlisten können im Einstellungen von AdBlock Plus unter dem Menüpunkt *Filter Preferences* abboniert werden. Hier ist der Menüpunkt *Filter -> Abonnement hinzufügen* zu wählen. Aus der Liste der angebotenen Filter können regional passende Listen gewählt werden. Folgende Filter-Listen sind als Ergänzung zur EasyList passend:

- **EasyPrivacy** blockiert meist unsichtbare Tracking-Elemente zum Ausspähen ihres Verhaltens im Internet mit HTML-Wanzen. Die Liste ist eine sinnvolle Ergänzung zur EasyList (Germany). Bei der Installation von *EasyPrivacy* kann die zusätzliche empfohlene EasyList deaktiviert werden, da sie bereits vorhanden ist.

- **Fanboy's Social Blocking List** ist eine Liste zum Blockieren der verschiedenen Social Media Tracking Features wie Facebook Like Buttons u.ä. Zur Installation kopiert man folgende URL in die Adressleiste von Firefox: abp:subscribe?location=https://easylist-downloads.adblockplus.org/fanboy-social.txt.

- **Anti-AdBlock Killer** blockiert die Scripte, die z.B. von Bild.de und anderen Webseiten des Springer-Verlags eingesetzt werden, um Surfer zur Deaktivierung der Werbeblocker zu zwingen. Damit kann man wieder überall werbefrei surfen. Zur Installation kopiert man folgende URL in die Adressleiste von Firefox:

abp:subscribe?location=https://raw.githubusercontent.com/reek/anti-adblock-killer/master/anti-adblock-killer-filters.txt.

Mit der Version 2.0 hat AdBlock Plus eine Whitelist für unaufdringliche Werbung eingeführt. Die Filterung wird auf den Webseiten in der Whitelist abgeschaltet, so dass diese Webseiten Werbung einblenden können. Wer auch keine unaufdringliche Werbung sehen möchte, kann dieses Feature wie in Bild 4.11 in der Übersicht der Filterlisten abschalten, indem man die Option *Nicht aufdringliche Werbung zulassen* deaktiviert.

Abbildung 4.11: Whitelisting in AdBlock Plus deaktivieren

Statt dessen kann man selbst entscheiden, welchen Webseiten man das Anzeigen von Werbung gestatten möchte. Mit einem gelegentlichen Klick auf Werbung kann man gute Webseiten bei der Finanzierung unterstützen. Wenn Sie eine Webseite im Browser geöffnet haben, können Sie in den Menü von AdBlock die aktuelle Webseite zu einer eigenen Whitelist hinzufügen.

4.7.5 Werbung auf der NewTab Page

Mozilla möchte die NewTab Seite für die Einblendung von Werbung nutzen. Diese Seite erscheint standardmäßig, wenn man einen neuen Tab öffnet. Sie soll Thumbnails der häufig genutzten Webseiten zeigen. Bei einem frisch installierten Browser oder wenn man die Speicherung der History deaktiviert, bleibt diese Seite allerdings leer.

Mozilla Chefin Mitchell Baker ist der Meinung[34], dass die Mehrzahl der Nutzer es gut finden oder es tolerieren werden, wenn die leeren Thumbnails

[34] http://heise.de/-2115431

für Werbung genutzt werden. Mit Firefox 33.1 hat Mozilla die Pläne zur Werbung auf der NewTab Seite umgesetzt.

Man kann die Werbung abschalten indem man auf das kleine Zahnrad oben rechts in der NewTab Seite klickt und in dem sich öffnenden Menü Abb. 4.12 die Option *Leere Seite anzeigen* auswählt. Wer an der NewTab Seite Gefallen gefunden hat und sie weiterhin nutzen möchte, sollte zumindest die Option *Vorschläge einbeziehen* deaktivieren.

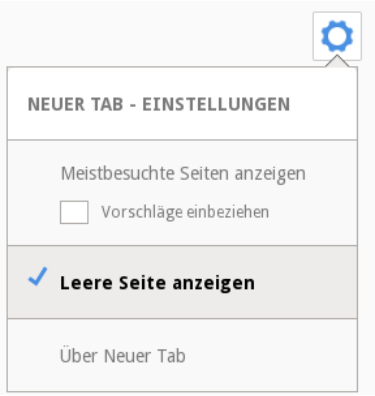


Abbildung 4.12: NewTab Seite konfigurieren

Speicherung von Screenshots der besuchten Webseiten

Firefox speichert Screenshots von jeder besuchten Webseite auf der Festplatte, um sie später als Thumbnails auf der New Tab Page einzublenden. Diese Speicherung gefällt mir nicht, da ich mein Surfverhalten nicht protokollieren möchte, auch nicht auf dem eigene Rechner. Um diese Speicherung abzuschalten, kann man eine neue Variable vom Typ Boolean unter *about:config* erstellen:

```
browser.pagethumbnails.capturing_disabled = true
```

Mozillas Werbung nach einem Update

Nach jedem Update von Firefox wird eine Webseite aufgerufen, die Mozilla für Werbung sowie statistische Auswertungen nutzt und die ein bisschen nervt. Unter der Adresse *about:config* kann man diese Einblendung abschalten:

```
browser.startup.homepage_override.mstone = "ignore"
startup.homepage_welcome_url             = " "
startup.homepage_welcome_url.additional  = " "
startup.homepage_override_url            = " "
```

4.8 History Sniffing

Browser speichern Informationen über besuchte Webseiten in einer Surf-History. Eine empirische Untersuchung der University of California [35] zeigt, dass ca. 1% der Top 50.000 Websites versuchen, diese Daten über zuvor besuchte Websites auszulesen. Daneben gibt es spezielle Anbieter wie Tealium oder Beencounter, die einem Webmaster in Echtzeit eine Liste der Websites liefern, die ein Surfer zuvor besucht hat. Die dabei übermittelten Informationen erlauben ein ähnlich detailliertes Interessenprofil zu erstellen, wie das Tracking über viele Websites. In der Regel werden die Informationen für die Auswahl passender Werbung genutzt.

Ein Experiment des Isec Forschungslabors für IT-Sicherheit [36] zeigt, dass diese History-Daten auch zur Deanonymisierung genutzt werden können. Anhand der Browser History wurde ermittelt, welche Gruppen bei Xing der Surfer bisher besucht hat. Da es kaum zwei Nutzer gibt, die zu den gleichen Gruppen gehören, konnte mit diesen Daten eine Deanonymiserung erfolgen. Die Realnamen sowie E-Mail Adressen konnten ohne Mithilfe der Surfer ermittelt werden.

In der Regel wurde der Besuch von Webseiten in der Vergangenheit durch Auswertung der Formatierung von Links ermittelt. Im Browser werden Links zu bereits besuchten Webseiten anders dargestellt, als unbekannte Webseiten. Deshalb hat Mozille 2010 die folgende Option eingeführt, mit der man die abweichende Formatierung von besuchten Links verhindern kann:

```
layout.css.visited_links_enabled = false
```

Seit 2013 ist Firefox auch in der Standardkonfiguration robust gegen diese Trackingmethode und verhindert das Auslesen der Formatierungen für die Darstellung besuchter Webseiten. Das Deaktivieren der Formatierung von besuchten Links ist daher als Verteidigung gegen Tracking nicht mehr nötig, kann aber Peinlichkeiten vor dem Bildschirm vermeiden.

Es wurde andere Angriffe auf die Surfhistory entwickelt (z.B. Timing Attacks). Die einzig wirksame Verteidigung besteht in der Deaktivierung der Surf-History. Im Dialog *"Einstellungen"* kann man auf dem Reiter *"Datenschutz"* die Speicherung besuchter Webseiten deaktivieren.

Außerdem können Webseiten in einem Tab die Anzahl der zuvor besucht Webseiten auslesen. Um das zu verhindern, kann man unter *about:config* folgenden Wert setzen:

```
browser.sessionhistory.max_entries = 2
```

Damit kann man aber mit dem Back-Button nur noch eine Seite zurück gehen. :-(

[35] http://cseweb.ucsd.edu/users/lerner/papers/ccs10-jsc.pdf
[36] http://www.iseclab.org/papers/sonda-TR.pdf

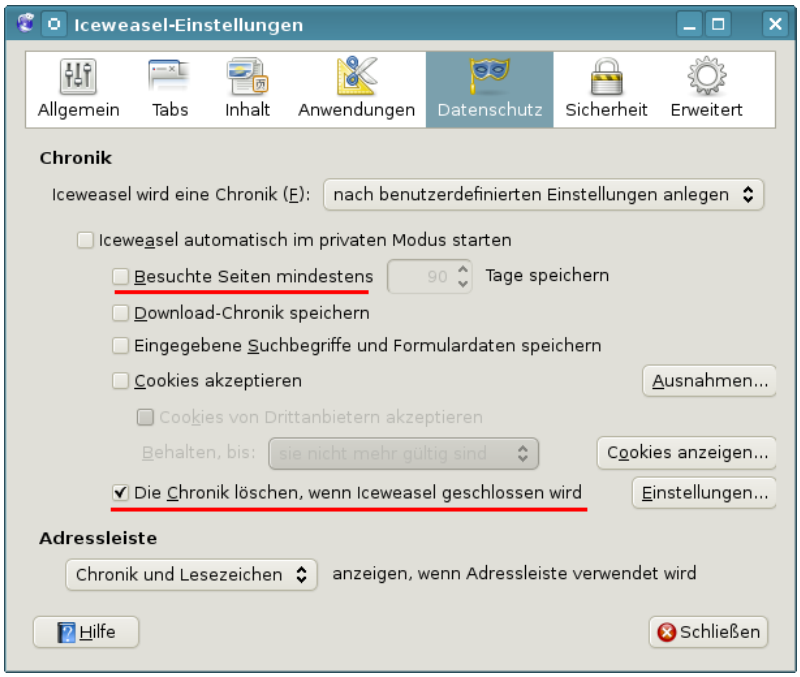


Abbildung 4.13: Speichern der Surf-Chronik deaktivieren

4.9 Browsercache und Chronik

Mit jeder aufgerufenen Webseite wird ein ETag gesendet, welches der Browser im Cache speichert. Wird die Webseite erneut aufgerufen, sendet der Browser zuerst das ETag, um zu erfragen, ob die Seite sich geändert hat. Dieses Tag kann eine eindeutige User-ID enthalten. KISSmetrics[37] verwendete diese Technik, um gelöschte Tracking-Cookies wieder herzustellen.

Ein vollständiges Abschalten des Cache ist nicht empfehlenswert. Man sollte den Cache des Browsers beim Schließen automatisch bereinigen. Im Firefox wird der Cache mit weiteren temporären Daten in der *Chronik* zusammengefasst. Die Einstellungen zum Löschen der Chronik findet man unter *Einstellungen* auf dem Reiter *Datenschutz*. Klicken Sie auf den Button *Einstellungen* hinter der Option *Die Chronik löschen, wenn Firefox geschlossen wird*. In dem sich öffnenden Dialog kann man detailliert festlegen, welche Daten beim Schließen des Browsers gelöscht werden sollen.

Alternativ kann man unter *about:config* folgende Werte setzen:

```
privacy.sanitize.sanitizeOnShutdown   = true
privacy.clearOnShutdown.cache         = true
privacy.clearOnShutdown.cookies       = true
privacy.clearOnShutdown.downloads     = true
```

[37] http://heise.de/-1288914

Abbildung 4.14: Cache löschen beim Beenden

```
privacy.clearOnShutdown.formdata      = true
privacy.clearOnShutdown.history       = true
privacy.clearOnShutdown.offlineApps   = true
privacy.clearOnShutdown.sessions      = true
privacy.clearOnShutdown.siteSettings  = true oder false
privacy.clearOnShutdown.openWindows   = false
```

Die erste Option aktiviert das Löschen der Chronik beim Schließen des Browsers. Die weiteren Parameter legen fest, welche Werte gelöscht werden sollen. *openWindows* sollte man auf FALSE setzen, da sonst evtl. immer zwei Instanzen des Browsers gestartet werden. Bei den *siteSettings* kann man überlegen, ob man alle Cookie Freigaben löschen möchte und gegen HSTS-Cookies geschützt sein möchte, oder ob man die Cookie Freigaben für ausgewählte Webseiten aus Bequemlichkeit lieber behält.

Während des Surfens kann man die Chronik mit der Tastenkombination STRG-SHIFT-ENTF löschen oder über *Extra - Neueste Chronik löschen*.

Firefox verwendet einen Cache im Hauptspeicher und einen Disk-Cache auf der Festplatte. Der Cache im Hauptspeicher ist mit 64 MB groß genug für eine Surf-Session. Den Disk-Cache kann man deaktivieren und damit auch überflüssige Spuren auf dem Rechner vermeiden, die forensisch sichtbar gemacht werden könnten. Unter *about:config* sind dafür folgende Variablen zu setzen:

```
browser.cache.disk.enable        false
browser.cache.disk_cache_ssl     false
browser.cache.offline.enable     false
media.cache_size                 0
```

4.10 Referer

Ein Referer liefert die Information, von welcher Seite der Surfer zu der aufgerufenen Webseite gekommen ist, oder bei der Einblendung von Werbung durch Dritte die Information, welche Seite er gerade betrachtet. Es ist ein sehr gut geeignetes Merkmal für das Tracking mit Werbung, HTML-Wanzen und Like-Button - die Schleimspur im Web.

Die Studie *Privacy leakage vs. Protection measures* [38] zeigt, dass außerdem viele Webseiten private Informationen via Referer an Trackingdienste übertragen. Das folgende Beispiel zeigt den Aufruf eines Werbebanners nach dem Login auf der Webseite http://sports.com

```
GET http://ad.doubleclick.net/adj/....
Referer: http://submit.sports.com/...?email=name@email.com
Cookie: id=123456789.....
```

Mit einer eindeutigen UserID (im Beispiel ein Tracking-Cookie) kann das Surfverhalten über viele Webseiten verfolgt werden. Durch zusätzliche Informationen (im Beispiel eine E-Mail Adresse) werden die gesammelten Datensätze personalisiert. Im Rahmen der Studie wurde 120 populäre Webseiten untersucht. 56% der Webseiten sendeten nach dem Login private Informationen wie E-Mail Adresse, Name oder Wohnort an Trackingdienste.

Firefox bietet die Möglichkeit, das Senden des Referers and Drittseiten zu blockieren. Dafür setzt man unter *about:config* folgende Option:

```
network.http.referer.XOriginPolicy = 2
```

Mit dieser Einstellung werden Subdomains als Drittseiten behandelt und es wird auch an Subdomains kein Referer gesendet. Das bringt möglicherweise vereinzelt Probleme bei einigen Websites mit sich. Anderseits schützt es gegen Trackingdienste, die sich mit DNS-Aliases als Subdomains auf populären Webseiten einschleichen wollen (z.B. WebTrekk bei Heise.de und Zeit.de).

Einige Webseiten zum Thema Privacy empfehlen, das Senden des Referers mit folgender Option komplett zu deaktivieren:

```
network.http.sendRefererHeader = 0
```

Wir empfehlen diese Einstellung nicht! Im Vergleich zu unserer Empfehlung verbessert es den Schutz gegen Tracking nicht. Innerhalb einer Domain kann der Webmaster einen Surfer immer verfolgen, mit oder ohne Referer. Die Einstellung führt statt dessen zu einem individuellen Fingerprint, da der Request-Header ganz ohne Referer sich von den 99% der anderen Surfer unterscheidet. Außerdem hat man öfters seltsame Probleme, weil Spam-Schutz Module in Diskussionsforen und Blogs oft den Referer als Feature zur Erkennung von Spam-Bots auswerten.

Alternativ kann man die Add-ons **Smart Referer** oder **Referrer Control** installieren. Mit dieses Add-ons können Ausnahmen vom Standardverhalten

[38] http://w2spconf.com/2011/papers/privacyVsProtection.pdf

definiert und spezifische Einstellungen für einzelne Websites konfiguriert werden. Nach der Installation der Add-ons kann man in den Einstellungen das Verhalten anpassen.

Technisch hochentwickelte Datensammler können den Schutz teilweise aushebeln indem der Referer zusätzlich in URL-Parametern übertragen wird.

4.11 Risiko Plugins

Für die Darstellung von Inhalten, die nicht im HTML-Standard definiert sind, kann Firefox Plug-ins nutzen. Populär sind Plug-ins für die Anzeige von PDF-Dokumenten im Browser oder Flash Videos. Die Nutzung dieser Plug-ins ist jedoch ein Sicherheitsrisiko.

Die Plug-ins können in der Add-on Verwaltung in der Sektion *Plugins* deaktiviert werden. Um zu verhindern, das bei der Installation von irgendwelchen Softwarepaketen ungewollt Browser Plug-ins automatisch aktiviert werden, kann man folgende Variable unter *about:config* setzen:

```
plugin.default.state = 0
```

Um unter Windows das automatische Scannen der Registry nach neuen Plug-ins zu deaktivieren, ist unter *about:config* folgende Variable zu setzen:

```
plugin.scan.plid.all = false
```

Außerdem kann man die Gefahr durch Plug-ins reduzieren, indem man sie erst nach Bestätigung laufen lässt:

```
plugins.click_to_play  =  true
```

Dann werden externe Plug-ins nur aktiviert, wenn der Nutzer es wirklich per Mausklick erlaubt und Drive-By-Download Angriffe sind nicht mehr möglich. Nur Flash-Applets werden weiterhin sofort ausgeführt. Diese Applets können mit dem Add-on NoScript blockiert und individuell mit einem Mausklick freigegeben werden.

4.11.1 PDF Reader Plugins

Anwender sind relativ unkritisch gegenüber PDF-Dokumenten. Was soll beim Anschauen schon passieren? Nur wenige Surfer wissen, dass es mit präparierten PDFs möglich ist, den *ZeuS-Bot* zu installieren und den Rechner zu übernehmen [39]. 2008 gelang es dem *Ghostnet*, die Rechnersysteme westlicher Regierungen, der US-Regierung und des Dalai Lama mit bösartigen PDFs zu infizieren [40]. 2012 gelang es dem Trojaner MiniDuke[41], mit bösartigen PDFs in die Computer von Regierungsorganisationen in Deutschland, Israel, Russland, Großbritannien, Belgien, Irland, Portugal, Rumänien, Tschechien

[39] http://heise.de/-979037
[40] http://www.linux-magazin.de/Heft-Abo/Ausgaben/2010/01/Geisterstunde
[41] http://heise.de/-1812971

und der Ukraine einzudringen. Über eine von Adobe als *nicht kritisch* eingestufte Sicherheitslücke einer überflüssigen PDF-Funktion wurde der Wurm *Win32/Auraax* verteilt [42]...

Nach Beobachtung des Sicherheitsdienstleisters Symantec[43] und ScanSafe[44] erfolgen die meisten Angriffe aus dem Web mit bösartigen PDF-Dokumenten. 2009 wurden für ca. 50% der Angriffe präparierten PDF-Dokumente genutzt (mit steigender Tendenz).

Schutzmaßnahmen:

1. Statt funktionsüberladener Monster-Applikationen kann man einfache PDF-Reader nutzen, die sich auf die wesentliche Funktion des Anzeigens von PDF-Dokumenten beschränken. Die FSFE stellt auf PDFreaders.org [45] Open Source Alternativen vor.
   - Für Windows werden *Evince* und *Sumatra PDF* empfohlen.
   - Für Linux gibt es *Okular* (KDE) und *Evince* (GNOME, XFCE, Unity).
   - Für MacOS wird *Vindaloo* empfohlen.
2. Wenn die PDF Reader Plugins nicht deinstallierbar sind (keine Adminstrator-Rechte), können sie im Browser deaktiviert werden. Diese Funktion finden Sie im Addon-Manager unter *Extras -> Add-ons*. PDF-Dokumente sollte man vor dem Öffnen zu speichern und nicht im Kontext des Browsers zu betrachten.
3. Außerdem sollte man PDF Dokumenten aus unbekannter Quelle ein ähnliches Misstrauen entgegen bringen, wie ausführbaren EXE- oder PAF-Dateien. Man kann einen Online-PDF-Viewer [46] nutzen, um PDF-Dokumente aus dem Internet zu betrachten ohne den eigenen Rechner zu gefährden.

4.11.2 Java-Applets

Es gibt eine Vielzahl von sinnvollen Java-Anwendungen. Im Internet spielt Java aber keine Rolle mehr (im Gegensatz zu Javascipt, bitte nicht verwechseln). Trotzdem installiert Oracles Java unter Windows ohne Nachfrage ein Browser-Plugin zum Ausführen von Java-Applets, die in Webseiten eingebettet sein können. Dieses Plug-in ist in erster Linie ein Sicherheitsrisiko und kann zur unbemerkten Installation von Trojanern genutzt werden.[47] [48] [49]

Der (Staats-) Trojaner der italienischen Firma *HackingTeam*[50] wird beispielsweise mit einer sauber signierten JAR-Datei auf dem Zielsystem installiert.

[42] http://heise.de/-990544
[43] http://heise.de/-981631
[44] http://www.scansafe.com/downloads/gtr/2009_AGTR.pdf
[45] http://www.pdfreaders.org/index.de.html
[46] http://view.samurajdata.se
[47] http://heise.de/-1485195
[48] http://heise.de/-1677249
[49] http://heise.de/-1780850
[50] http://heise.de/-1671203

Der Trojaner belauscht Skype, fängt Tastatureingaben ab, kann die Webcam zur Raumüberwachung aktivieren und den Standort des Nutzers ermitteln.

Als Schutz wird häufig die die komplette Deinstallation von Java empfohlen (BSI[51], DHS[52], Fefe[53]). Das ist Bullshit und nur sinnvoll, wenn man keine Java-Programme nutzt. Anderenfalls ist die komplette Deinstallation von Java eine unnötige Einschränkung für sinnvolle Anwendungen.

- Aktuelle **Linux** Distributionen verwenden in der Regel OpenJDK-6/7. Diese Java-JRE installiert KEIN Browser Plug-in. Es besteht also auch keine Gefahr, durch bösartige Java-Applets aus dem Internet den Rechner zu verseuchen.

- Unter **Windows** bietet die aktuelle Version von Oracles Java die Möglichkeit, die Plug-ins für alle Browser unter *Systemsteuerung - Programme - Java* zu deaktivieren (Bild 4.15).

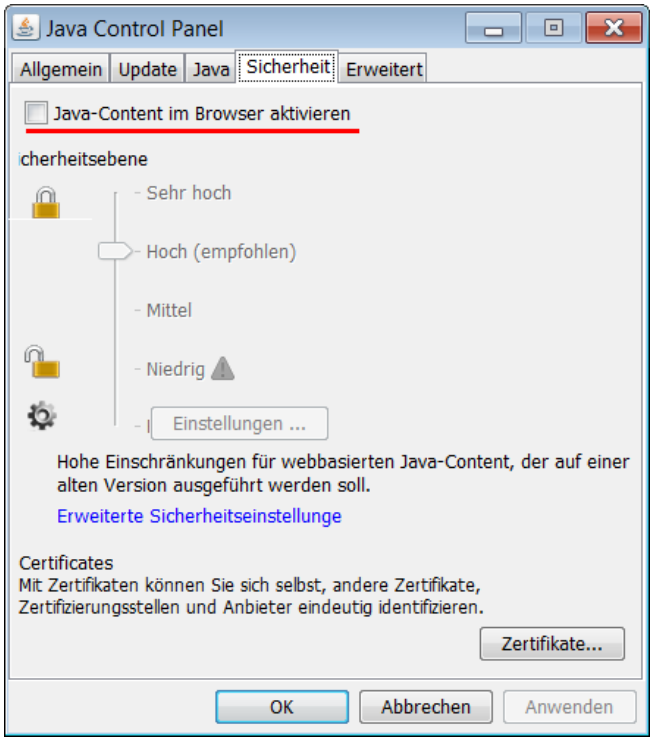


Abbildung 4.15: Java Plug-in für alle Browser deaktivieren

[51] https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2013/Krit_Schwachstelle_Java-7-10_11012013.html
[52] http://www.nbcnews.com/technology/technolog/us-warns-java-software-security-concerns-escalate-1B7938755
[53] https://blog.fefe.de/?ts=ae0f1f75

4.11.3 Flash-Applets und Flash-Videos

Flash Applets sind ein Sicherheits- und Privacyrisiko. Diese Applets können umfangreiche Informationen über den Browser auslesen (installierte Schriftarten, Betriebssystem, Kernelversion) und daraus einen genauen Fingerprint zum Tracking berechnen. Die Studie *Dusting the Web for Fingerprinters* der KU Leuven (Belgien) hat bei 1% der TOP 10.000 Webseiten Flash-basiertes Fingerprinting des Browsers nachgewiesen.

Die italienische Firma Hacking Team verwendete mindestens drei Bugs im Flash Player für 0day Exploits, um ihre Spionage Software als Drive-by-Download auf den Computern der Opfer zu installieren.[54]

Auch bei Cyber-Kriminellen ist Flash sehr beliebt. Die Firma F-Secure hat analysiert, welche Lücken von den bekannten Exploits-Kits am häufigsten genutzt werden. Unter den 15 am häufigsten verwendeten Lücken findet man 13x den Flash Player.[55]

Verwendung von Flash vermeiden

1. Flash-Player deinstallieren!

2. Das Firefox Add-on **VideoDownloadHelper** [56] kann man Videos von vielen Websites herunter laden und in ein gebräuchlicheres Format für Mediaplayer konvertieren. Wer noch keinen passenden Mediaplayer installiert hat, kann den VideoLAN Player nutzen (VLC-Player), der für alle Betriebssysteme zur Verfügung steht.

   Für die volle Funktionalität benötigt das Add-on die Bibliothek *Libav* für die Konvertierung von Videos. Diese Bibliothek ist zusätzlich zu installieren:

   - Für Windows findet man ein Installationspaket auf der Webseite http://www.downloadhelper.net/install-converter3.php
   - Debian Nutzer können *Libav* aus dem Repository installieren:

     ```
     > sudo apt install libav-tools libavcodec-extra-56
     ```

   - Für Ubuntu und abgleitet Distributionen installiert man die nötigen Pakte mit:

     ```
     > sudo apt install libav-tools libavcodec-extra chromium-codecs-ffmpeg-ex
     ```

   - Unter MacOS ist ein Terminal zu öffnen, um mit Homebrew die Libav zu installieren:

     ```
     brew install libav
     ```

[54] http://blog.trendmicro.com/trendlabs-security-intelligence/unpatched-flash-player-flaws-more-pocs-found-in-hacking-team-leak/
[55] https://business.f-secure.com/have-you-disabled-flash-yet
[56] https://addons.mozilla.org/de/firefox/addon/video-downloadhelper

3. Web Videos können mit Hilfe von Download Sites wie KeepVid [57] oder ShareTube [58] gespeichert und mit einem Mediaplayer abgespielt werden.

Privacy-freundliche Konfiguration für Adobe Flash-Player

Wenn man auf Flash im Browser nicht verzichten kann, dann sollte man in der Plug-in Verwaltung den Status für das Plug-in in jedem Fall auf *Ask to Activate* stellen, damit keine bösartigen Applets oder Tracking Applets unbemerkt im Hintergrund ausgeführt werden. Alternativ kann man Flash-Applets auch mit dem Add-on NoScript blockieren. NoScript zeigt einen Platzhalter an und man kann das Applet mit einem Klick bei Bedarf aktivieren.

Wenn man auf Flash nicht verzichten möchte, kann man mit der Konfigurationsdatei *mms.cfg* ein privacy-freundlicheres Verhalten für den Adobe Flash-Player erzwingen und einige Trackingfeatures deaktivieren. Die Datei ist in folgenden Verzeichissen zu speichern:

```
Windows (32Bit): %Windir%\System32\Macromed\Flash\
Windows (64Bit): C:\Windows\SysWOW64\Macromed\Flash\
MacOS:          /Library/Application Support/Macromedia/
Linux:         /etc/adobe/
```

Folgende Optionen empfehle ich für die Konfigurationsdatei *mms.cfg*:

- Deaktivierung von Mikrofon und Lautsprecher sowie Abschaltung des Auslesens der Schriftarten erschweren Fingerprinting des Browsers:

  ```
  AVHardwareDisable=1
  DisableDeviceFontEnumeration=1
  ```

- Blockierung der Speicherung von Cookies und Drittseiten-Content verhindert Tracking:

  ```
  ThirdPartyStorage=0
  LocalStorageLimit=1
  AssetCacheSize=0
  ```

- Up- und Download von Dateien mit der Scripting API wird blockiert:

  ```
  FileDownloadDisable=1
  FileUploadDisable=1
  LocalFileReadDisable=1
  ```

- Für die gemeinsame Nutzung von SWF-Dateien in einer Sandboxen wird die exakte Übereinstimmung der Domains erzwungen und die lockeren Einstellungen von Flash Player Version 6.0 werden verboten:

  ```
  LegacyDomainMatching=0
  ```

[57] http://keepvid.com
[58] http://www.share-tube.de/flvdownload.php

- Deaktivierung von Sockets verhindert die Deanonymisierung durch Umgehung der Proxy-Einstellungen des Browsers bei der Nutzung von Anonymisierungsdiensten wie JonDonym oder Tor:

  ```
  DisableSockets=1
  ```

Damit werden nicht alle Fingerprinting-Features deaktiviert. Betriebssystem, Kernel, Bildschirm und Systemzeit sind weiterhin auslesbar, aber es ist eine deutliche Verbesserung.

4.11.4 Weitere Anwendungen

Neben PDF-Dokumenten können auch alle anderen Dokument-Typen für Drive-by-Donwload Angriffe verwendet werden. Um diese zu unterbinden, sollte man externe Anwendungen für Dateien nur nach Bestätigung durch den Anwender öffnen lassen. Anderenfalls können Bugs in diesen Anwendungen automatisiert genutzt werden.

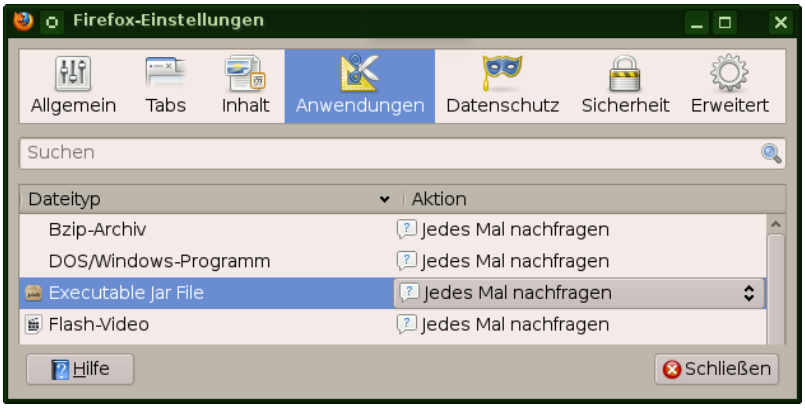


Abbildung 4.16: Externe Anwendungen nur auf Nachfrage öffnen

Auf dem Reiter *Anwendungen* im Dialog *Einstellungen* können die Helper-Applications wie im Bild 4.16 für jeden Dateityp auf *"Jedes Mal nachfragen"* gesetzt werden. Diese Einstellungen sind natürlich nur sinnvoll, wenn der Surfer kritisch hinterfragt, ob die Aktion wirklich dem entspricht, was er erwartet. Wer unkritisch bei jeder Nachfrage auf *Öffnen* klickt, muss sich nicht wundern, wenn sein Computer infiziert wird.

4.11.5 H.264 Plug-in und Adobe Primetime deaktivieren

Der H.264-Codec für WebRTC und HTML5 Videos wird als Closed Source Plug-in von Cisco herunter geladen und automatisch installiert. Man kann die automatische Installation des Plug-in verhindern, wenn man unter *about:config* folgende Werte auf false setzt:

```
media.gmp-gmpopenh264.enabled          = false
media.gmp-provider.enabled = false
```

Adobe Primetime ist ein Plug-in zur Wiedergabe von DRM-geschützten Inhalten. Es ist im Firefox 38.0 für Windows standardmäßig enthalten. Ein Plug-in von Adobe ist etwas, was ich aus Sicherheitsgründen auf keinen Fall in meinem Browser haben möchte. Mozilla beschreibt in einem Artikel [59], wie man das Plug-in entfernt. Unter *Einstellungen* in der Sektion *Inhalt* ist die Option *Inhalte mit DRM-Kopierschutz wiedergeben* zu deaktivieren.

Abbildung 4.17: Adobe Primetime deinstallieren

4.12 HTTPS-Verschlüsselung nutzen

Viele Websites bieten HTTPS-Verschlüsselung an. Diese sichere Datenübertragung wird häufig nicht genutzt. Mit wenig Konfigurationsaufwand lässt sich die Nutzung von HTTPS für eine definierte Liste von Websites erzwingen.

Firefox enthält eine *HSTS preload list*[60] mit mehr als 1200 Domains, für die HTTPS ohne weitere Konfiguration erzwungen wird. Webmaster können ihre Websites auf der Seite HSTS Preload Submission[61] eintragen, wenn sie die Voraussetzungen erfüllen.

NoScript Enforce HTTPS

NoScript Enforce HTTPS ist einfach konfigurierbar, kann aber nur *http://* durch *https://* für eine Liste von Websites ersetzen. Die Liste muss man per Hand erstellen. Im Dialog *Einstellungen* findet man auf dem Reiter *Erweitert* unter *HTTPS* eine editierbare Liste von Websites.

[59] https://support.mozilla.org/de/kb/drm-inhalte-in-firefox-ansehen
[60] https://mxr.mozilla.org/mozilla-central/source/security/manager/boot/src/nsSTSPreloadList.inc
[61] https://hstspreload.appspot.com/

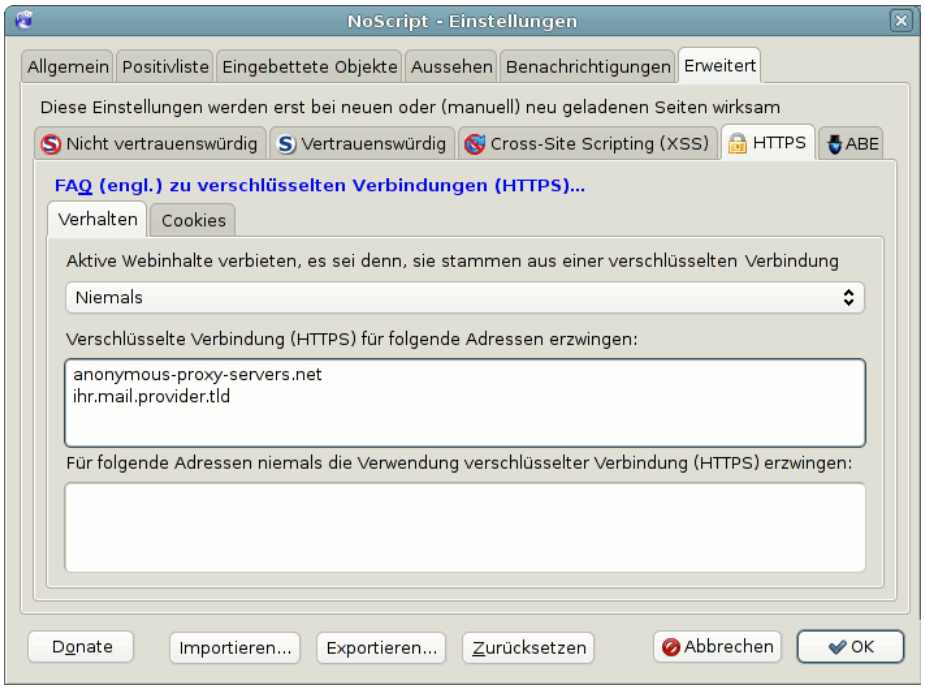


Abbildung 4.18: Einstellungen für NoScript STS

Standardmäßig ist die Liste leer. Wer das Webinterface eines E-Mail Providers nutzt, sollte die Domain hier eintragen. Außerdem sollte man die Webseite der Bank eintragen, wenn man Online-Banking nutzt und die Webseite nicht in HTTPSEverywhere oder der *HSTS preload list* enthalten ist.

HTTPS-Everywhere

Das Firefox Add-on HTTPS-Everywhere[62] der EFF.org kann auch komplexe Umschreibungen der URLs realisieren, wie es beispw. für Wikipedia notwendig ist. Das Add-on bringt bereits über 2500 Regeln für häufig genutzte Webseiten mit. Die Konfiguration eigener Regeln ist aufwendiger als bei NoScript und erfolgt über XML-Dateien.

Bei HTTPS-Everywhere sind Regeln standardmäßig deaktiviert, wenn der Server ein SSL-Zertifikat von CAcert.org nutzt (z.B www.ccc.de) Wenn Sie das Root-Zertifikat von CAcert.org im Browser importiert haben, dann können Sie diese Regeln in den Einstellungen von HTTPS-Everywhere mit Klick auf das Kreuz aktivieren (Bild 4.19).

[62] https://www.eff.org/https-everywhere

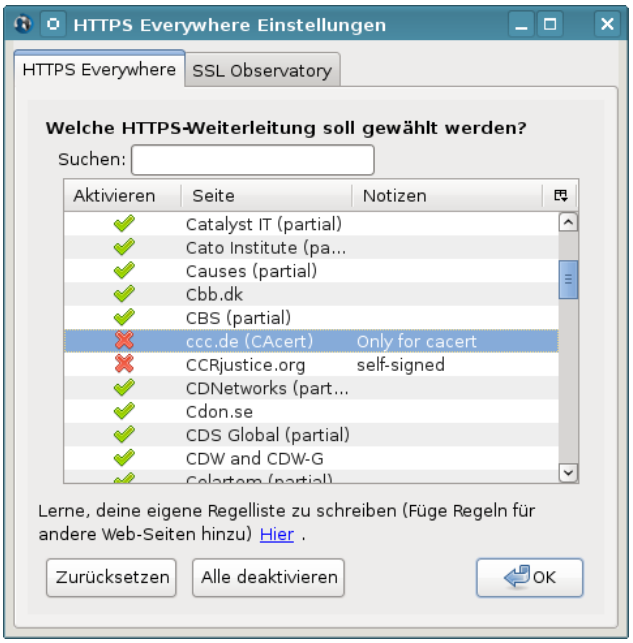


Abbildung 4.19: Einstellungen für Https-Everywhere

4.13 Vertrauenswürdigkeit von HTTPS

IT-Sicherheitsforscher der EFF kamen breits 2009 in einer wiss. Arbeit zu dem Schluss, dass Geheimdienste mit gültigen SSL-Zertifikaten schwer erkennbare man-in-the-middle Angriffe durchführen können. Diese Angriffe können routinemäßig ausgeführt werden, schreibt die [63]

> *Certificate-based attacks are a concern all over the world, including in the U.S., since governments everywhere are eagerly adopting spying technology to eavesdrop on the public. Vendors of this technology seem to suggest the attacks can be done routinely.*

Anbieter von fertige Appliances für diesen auch als *Lawful SSL Interception* bezeichneten Angriff findet man beim Stöbern in den SpyFiles von Wikileaks. Für staatliche Schnüffler gibt es mehrere Möglichkeiten, um diese Technik mit gültigen SSL-Zertifikate für schwer erkennbare man-in-the-middle Angriffe zu kombinieren:

1. Für einen großflächiger Angriff gegen iranische Internet Nutzer wurden im August 2011 mehrere CAs gehackt, um gültige SSL-Zertifikate zu erstellen (DigiNotar, Comodo, InstantSSL und zwei Sub-Registrare von Comodo). Bei DigiNotar wurden 531 Zertifikate kompromittiert. Neben den Webseiten von Google, Yahoo, Mozilla, Skype, TorProject.org u.a. waren auch die Webdienste von MI6, CIA und Mossad betroffen.

[63] https://eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl

2. Certification Authorities könnten unter Druck gesetzt werden, um staatlichen Stellen SubCA-Zertifikate auszustellen, mit denen die Zertifikate für man-in-the-middle Angriffe signiert werden könnten. Ein Kommentar zum TürkTRUST Desaster von Adi Shamir:

   > *I think you will see more and more events like this, where a CA under pressure from a government will behave in strange ways.*

   Im Juni 2014 signierte die staatliche indische Certification Authority (NIC) gefälschte SSL-Zertifikate für Google Dienste und Yahoo!. 45 gefakte Zertifikate wurden nachgewiesen. Ob es um eine staatliche Überwachung, einen Hackerangriff oder einen Konfigurationsfehler(?) handelt, ist unklar.[64].

3. Die Anbieter von Webdiensten können zur Herausgabe der eigenen Zertifikate und Keys gezwungen werden, wie am Beispiel des E-Mail Providers Lavabit bekannt wurde. Die betroffenen Provider sind zum Stillschweigen verpflichtet. Der Angreifer kann mit diesen Zertifikate einen Angriff auf die SSL-Verschlüsselung durchführen, der nicht mehr erkennbar ist.

4. Verisign ist nicht nur die größte Certification Authority. Die Abteilung NetDiscovery von Verisign ist ein Global Player in der Überwachungstechnik und unterstützt die Behörden und westliche Geheimdienste seit 2002 bei SSL Interception.

Kriminelle Subjekte haben ebenfalls nachgewiesen, dass sie für man-in-the-middle Angriffe auf die SSL-Verschlüsselung gültige Zertifikate verwenden können (bspw. beim Angriff auf das Bitcoin Forum). Man kann sich so einfach als Unberechtigter ein gültiges SSL-Zertifikat für einen Server ausstellen zu lassen, wenn man die richtigen Mail-Account kontrolliert. Für die Ausstellung Domain-validierte SSL-Zertifikate werden die E-Mail Adressen *webmasterdomain.tld, postmasterdomain.tld, ssladmindomain.tld, ssladministratordomain.tld* u.a.m. u.a. akzeptiert. Eine unverschlüsselte E-Mail mit einem Verification Link an eine der genannten E-Mail Adressen ist die einzige Prüfung auf Rechtmäßigkeit durch die CAs.

Die Software für einen man-in-the-middle Angriff mit den gefälschten Zertifikaten gibt es auch als Open Source, z.B. den mitm-proxy[65] der Stanford University oder dsniff [66].

4.13.1 Verbesserung der Vertrauenswürdigkeit von HTTPS

Es gibt einige Möglichkeiten, die Vertrauenswürdigkeit der HTTPS-Verschlüsselung zu verbessern und Angriffe mit falschen Zertifikaten zu erschweren.

- **Zertifikate speichern:** Beim ersten Besuch der Webseite wird das SSL-Zertifikat gespeichert. Bei späteren Besuchen wird das aktuelle Zertifikat

[64] http://heise.de/-2255992
[65] http://crypto.stanford.edu/ssl-mitm/
[66] http://www.monkey.org/ dugsong/dsniff/

mit dem gespeicherten Zertifikat verglichen. Bei seltsamen Abweichungen wird eine Warnung angezeigt, die der Surfer allerdings bewerten muss.

- **Vergleich mit Anderen:** Beim Besuch einer HTTPS-verschlüsselten Webseite wird das Zertifikat mit den Ergebnissen an anderen Punkten der Welt verglichen. Wenn alle Teilnehmer des Netzes das gleiche Zertifikat sehen, ist es wahrscheinlich Ok. Dieser Vergleich kann mit einer zeitlich begrenzten Speicherung kombiniert werden.

  Obwohl die Idee auf den ersten Blick einleuchtend ist, gibt es einige Probleme bei großen Serverfarmen wie Google, Facebook, Amazon, PayPal... Diese Serverfarmen verwenden nicht immer ein einheitliches Zertifikat. Das führt zu Verwirrung bei einem externen Beobachter und zu inkonsistenten Ergebnissen der Notary Server.

- **Certificate Pinning:** Nur der Betreiber einer Webseite kann wirklich wissen, welche Zertifikate gültig sind. Diese Information muss unabhängig vom Webserver verteilt und durch die Browser ausgewertet werden. Das ist ein besserer Weg, als der Vergleich mit externen Beobachtern oder der Speicherung in einer lokalen Datenbank.

  - Nur der Betreiber einer Webseite kann wirklich wissen, welche Zertifikate gültig sind. Diese Information muss unabhängig vom Webserver verteilt und durch die Browser ausgewertet werden. Das ist ein besserer Weg, als der Vergleich mit externen Beobachtern oder der Speicherung in einer lokalen Datenbank.
  - DANE ist ein Standard, der im Januar 2014 verbschiedet wurde. Die Fingerprints der SSL-Zertifikate werden vom Webmaster im TLSA-Record via DNSSEC verteilt. Inzwischen gibt es einige Webseiten, die DANE anbieten. Um die Zertifikate zu verifizieren benötigt man ein zusätzliches Browser Add-on (z.B. den DNSSEV/TLSA-Validator), da die aktuellen Webbrowser das (noch) nicht selbst können.

4.13.2 Firefox Add-ons

Ein paar kleine Erweiterungen für Firefox, welche die Vertrauenswürdigkeit der Zertifikate bei der Nutzung von HTTPS-verschlüsselten Verbindungen deutlich erhöhen können.

DNSSEC/TLSA-Validator

DNSSEC/TLSA-Validator[67] überprüft die Zertifikate einer Webseite anhand der Fingerprints, die vom Webmaster im TLSA-Record in DNSSEC hinterlegt wurden. Der verwendete Standard DANE wurde im Januar 2014 verabschiedet und die ersten Anbieter unterstützen diese Verifikation, die unabhängig

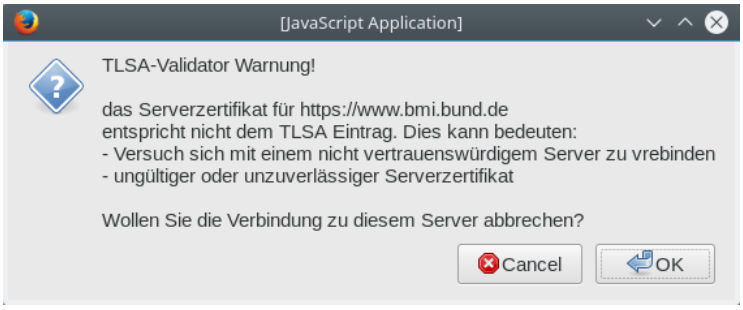
[67] https://www.dnssec-validator.cz/pages/download.html

von einer kompromittierbaren Certification Authority arbeitet.

Es werden zwei zusätzliche Icons in der Adresszeile angezegt. Normalerweise wird man folgendes Bild mit zwei grauen Icons sehen, weil die Webseite DANE noch nicht für die Valdierung der Zertifikate unterstützt:

Wenn ein TLSA-Record vom Webmaster im DNS hinterlegt wurde, dann sieht man zwei grüne Icons, wenn alles Ok ist. Wenn eines der beiden Icons orange ist, dann läuft etwas schief und man sollte dem SSL-Zertifikat NICHT vertrauen.

Standardmäßig zeigt das Add-on das Ergebnis der Validierung nur in der Adressleiste an. Die Webseite wird trotzdem geladen. Unter Umständen könnten damit bereits Daten komprottiert sein. Man kann in den Einstellungen des Add-ons den Sicherheitslevel verschärfen, indem man jeden Request validiert und bei Problemen die Verbindung abbricht. Dann zeigt das Add-on eine Warnung, bevor die Webseite geladen wird. (Man muss auf *Ok* klicken um das Laden abzubrechen!)



(Im vorliegenden Fehlerbeispiel wurde das SSL-Zertifikate für die Domain *www.bmi.bund.de* erneuert und die Anpassung des DANE/TLSA Record im DNS vergessen. Auch das passiert gelegentlich, nicht jeder Fehler ist ein Angriff auf die Verschlüsselung.)

Unbedingt: DNS-Server in den Einstellungen des Add-ons TESTEN. Wenn nötig kann man in den Einstellungen des Add-on einen anderen DNS-Server wählen, der DNSSEC unterstützt.

HTTPSEverywhere

HTTPS-Everywhere[68] kann das SSL-Obervatory der EFF.org nutzen. Wenn man diese Funktion in den Einstellungen des Add-on aktiviert, werden die SSL-Zertifikate der besuchten Webseiten an das SSL-Observatory gesendet. Ist das Zertifikat nicht ok, erhält man eine Warnung. Es wird eine Datenbasis von

[68] https://www.eff.org/https-everywhere

weltweit verteilten Nutzern genutzt.

HTTPSEverywhere ignoriert die Proxy-Einstellungen von Firefox. Wenn man einen Proxy konfiguriert hat, dann muss man unter *about:config* auch die folgenden Einstellungen für HTTPSEverywhere per Hand anpassen:

```
extensions.https_everywhere._observatory.proxy_type = direct | socks | http
extensions.https_everywhere._observatory.proxy_host = <IP oder Hostname>
extensions.https_everywhere._observatory.proxy_port = <Port des Proxy>
```

Hinweis: Im TorBrowserBundle muss man sich nicht darum kümmern, da das Add-on fester Bestandteil des TorBrowsers ist und die Proxy-Einstellungen natürlich fertig konfiguriert sind.

Perspectives

Perspectives[69] vergleicht SSL-Zertifikate mit den bei Notary Servern bekannten Zertifikaten. Wenn alle Notary-Server das gleiche Zertifikat über einen längeren Zeitraum sehen, ist es wahrscheinlich gültig. Leider gibt es noch nicht viele, international verteilte Notary Server. Alle standardmäßig im Add-on enthaltenen Server werden vom MIT bereit gestellt.

Aufgrund der nicht immer eindeutigen Resultate und der Performance der Notary Server ist Perspectives nicht unbedingt für eine ständige Validierung aller SSL-Zertifikate geeignet. Der Server awxcnx.de ist im Moment nur bei der Hälfte der Notary Server bekannt. Das führt zu einem Fehler bei Perspectives, obwohl eigentlich alles Ok ist.

Ich empfehle daher die Abfrage der Notarys bei Bedarf (wenn man ein Zertifikat genauer prüfen möchte). Dafür sind die Einstellungen in den Preferences wie im Bild 4.20 zu setzen.

Zukünftig kann man mit einem Klick der rechten Maustatste auf das Perspectives-Symbol in der Statusleiste einen Check des Zertifikates der Webseite erzwingen und sich die Notary Results anzeigen lassen.

4.13.3 SSL-Zertifikate via OCSP validieren

Das Online Certificate Status Protocol (OCSP) sollte eine Überprüfung der SSL-Zertifikate ermöglichen. Bevor der Browser eine SSL-Verbindung akzeptiert, fragt er bei der Certification Authority nach, ob das verwendete Zertifikat für diesen Server noch gültig ist. Um SSL-Zertifikate via OCSP zu verifizieren, wurden zwei Verfahren definiert:

OCSP.Get ist veraltet und leicht auszutricksen, wie Moxie Marlinspike in dem Paper *Defeating OCSP With The Character 3* (2009) gezeigt hat. Gängige Tools für Man-in-the-middle Angriffe wie sslsniff können das

[69] https://addons.mozilla.org/en-US/firefox/addon/perspectives/

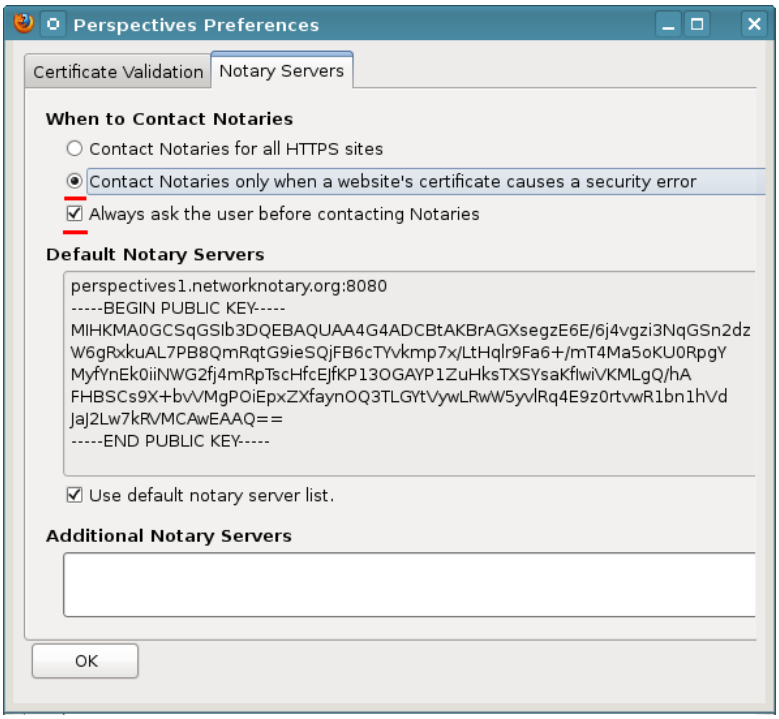


Abbildung 4.20: Perspectives Konfiguration

automatisiert ausführen. OCSP bringt also kaum Sicherheitsgewinn.[70]

Einige CAs nutzen die OCSP-Anfragen zum Tracking des Surfers mit Cookies, wie der folgende Mitschnitt eines OCSP-Request zeigt:

```
POST http://ocsp2.globalsign.com/gsorganizationvalg2 HTTP/1.1
Host: ocsp2.globalsign.com
User-Agent: Mozilla/5.0 (...) Gecko/20130626 Firefox/17.0 Iceweasel/17.0.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
Content-Length: 117
Content-Type: application/ocsp-request
Cookie: __cfduid=57a288498324f76b1d1373918358
```

Auch wenn aktuelle Browser keine Cookies von OCSP.Get Antworten mehr akzeptieren, erhält die Certification Authority (CA) laufend Informationen, von welcher IP-Adresse die SSL-geschützten Webseiten bzw. Mailserver o.ä. kontaktiert wurden. Da die OCSP-Anfrage und Antworten unverschlüsselt übertragen werden, kann auch ein *Lauscher am Draht* diese Informationen abgreifen.

[70] http://www.thoughtcrime.org/papers/ocsp-attack.pdf

OCSP.Stapling ist ein modernes Verfahren, dass die oben genannten Probleme vermeidet. Der Browser ruft ein Token vom Webserver ab, das die Gültigkeit des Zertifikates für einen kurzen Zeitraum bestätihgt und von der CA signiert wurde.

Moderne Webserver und alle akruellen Browser unterstützen es inzwischen. Der bekannte Test für Webserver Qualsys SSL Labs wird ab Jan. 2017 die Bestnote A+ nur vergeben, wenn der Webserver OCSP.Stapling anbietet. Die BSI Richtline TR-03116-4 (Kryptografische Vorgaben für TLS, S/MIME, OpenPGP und SAML) fordert ebenfalls Support für OCSP.Stapling. Somit wird sich das Verfahren weiter verbreiten.

Aktuelle Firefox Versionen sind sinnvoll vorkonfiguriert. Es wird standardmäßig nur OCSP.Stapling genutzt:

```
security.OCSP.enabled                  = 1
security.OCSP.GET.enabled              = false
security.ssl.enable_ocsp_stapling      = true
security.ssl.enable_ocsp_must_staple   = true
```

Zusätzlich kann man die Sicherheitseinstellungen verschärfen, indem man erzwingt, dass die OCSP Antworten gültig sein müssen, wenn der Webserver OCSP.Stapling unterstützt.

```
security.OCSP.require  = true
```

Falls man eine Webseite mit diesen Einstellungen temporär nicht aufrufen kann, dann muss es nicht am Webserver liegen. Möglicherweise hat der Server der CA Schluckauf und der angefragte Webserver kann das OCSP-Token nicht von der CA bekommen. Wenn es dringend ist und man außerdem DANE/TLSA zur Verifizierung des SSL-Zertifikates nutzt, kann man OCSP temporär deaktivieren. Wenn es nicht dringend ist, wartet man ein bisschen.

4.13.4 Tracking via SSL Session

Beim Aufbau einer verschlüsselten HTTPS-Verbindung zwischen Browser und Webserver wird eine sogenannte Session initialisert. Diese Session kann für 48h genutzt werden. Das beschleunigt das Laden der Webseite bei erneutem Zugriff, da die Details der Verschlüsselung nicht jedes mal neu zwischen Browser und Webserver ausgehandelt werden müssen. Da diese Session eindeutig ist, kann sie für das Tracking genutzt werden. Das Verfahren ist im RFC 5077 [71] beschrieben.

Die SSL-Session-ID kann von nahezu allen Webserven für das Tracking der Zugriffe genutzt werden. IBM WebSphere, Apache und andere bieten eine API für den Zugriff auf die SSL Session-ID. Einige Webshops sind für das Tracking via SSL Session-ID vorbereitet (z.B. die *xtcModified eCommerce Shopsoftware*[72]). Dieses Tracking-Verfahren ist so gut wie nicht nachweisbar, da es vollständig

[71] https://tools.ietf.org/html/rfc5077
[72] http://www.modified-shop.org/wiki/SESSION_CHECK_SSL_SESSION_ID

durch den Webserver realisiert wird und keine Spuren im Browser hinterlässt.

Gegen das Tracking via SSL Session Identifiers kann man sich ab **Firefox 36.0** schützen, indem man unter *about:config* eine neue Variable vom Type *Boolean* anlegt:

```
security.ssl.disable_session_identifiers = true
```

4.13.5 Tracking via HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) wurde als Schutz gegen den *ssl-stripe* Angriff eingeführt, den Moxie Marlinspike auf der Black Hack 2009 vorstellte. Der Angriff wurde beispielsweise 2012 von mehreren Bad Tor Exit Nodes aktiv genutzt.

Als Schutz gegen *ssl-stripe* Angriffe sendet der Webserver beim Aufruf einer Webseite einen zusätzlichen HSTS-Header, um dem Browser mitzuteilen, dass diese Website für eine bestimmte Zeit immer via HTTPS aufgerufen werden soll. Das verhindert ein Downgrade auf unverschlüsselte HTTP-Verbindungen.

S. Greenhalgh hat ein Verfahren publiziert, wie man HSTS für das Tracking von Surfern verwenden kann[73]. Es steht eine Testseite für HSTS Super-Cookies bereit, die dieses Verfahren demonstriert. Ob man HSTS im Browser deaktiviert, um sich gegen ein bisher nur theoretisch relevates Trackingverfahren zu schützen, oder ob man HSTS aktiviert, um sich gegen *ssl-stripe* Angriffe zu schützen (Standard im Firefox), ist also eine Wahl zwischen Skylla und Charybdis.

Meine Überlegungen dazu:

- In der Regel nutzt man nur eine begrenzte Anzahl von Websites regelmäßig, bei denen sensitive Informationen durch SSL-Verschlüsselung wirklich geschützt werden müssen (E-Mail Provider, Website der Bank, Diskussionsforen, bevorzugte Suchmaschine....). Mit der HSTS preload list, NoScript oder HTTSEverywhere kann man SSL-Verschlüssung für diese Websites erzwingen und ist damit auch ohne HSTS gegen *ssl-stripe* Angriffe geschützt.
- Unter der Adresse *about:config* kann man folgende Variable setzen:

  ```
  privacy.clearOnShutdown.siteSettings = true
  ```

  Damit werden beim Schließen des Browsers alle gespeicherten HSTS-Werte gelöscht und ein langfristiges Tracking wird verhindert. Während einer Surf-Session ist der HSTS-Schutz aktiv.
- Innerhalb einer Surf-Session kann man HSTS-Cookies mit der Tastenkombination STRG-SHIFT-ENTF löschen. Zum Löschen der HSTS-Werte ist unter Details die Option *Website-Einstellungen* zu aktivieren.

[73] http://heise.de/-2511258

4.13.6 SSL/TLS Konfiguration

Die SSL-Verschlüsselung ist ein komplexer Standard, der über Jahre gewachsen ist. Neben aktuell starken Algorithmen sind auch schwache kryptografische Verfahren enthalten, die aus Kompatibilitätsgründen unterstützt werden:

1. Das Protokoll SSLv3 ist geknackt. Mozilla hat SSLv3 in Firefox 34 standardmäßig abgeschaltet.

2. Die RC4-Cipher sind schwach und genügen aktuellen Anforderungen nicht mehr. Laut Empfehlung der IETF (RFC 7465) darf RC4 nicht mehr für die Verschlüsselung genutzt werden und ist in Firefox seit Version 44 deaktiviert.

3. Für die 3DES-Verschlüsselung gibt es mit der Birthday Attack einen plausiblen Angriff der allerdings im Moment noch große Datenmengen > 32GB erfordert. Diese Cipher sollten aber ebenfalls deaktiviert werden. Krypto-Experten empfehlen, 3DES wie RC4 zu behandeln und in den Standards die Nutzung zu verbieten. Derzeit wird 3DES in Firefox noch unterstützt.

4. Beim Diffie-Hellman-Schlüsseltausch kann der Admin viele Fehler bei der Konfiguration des Webservers machen. Auf der Webseite https://badssl.com kann man ausprobieren, dass Firefox diese Schwächen nicht erkennt und schwache DH-Parameter für den Schlüsseltausch aktzeptiert. Außerdem muss man davon ausgehen, dass die NSA die Common DH Primes lt. RFC 2409 bis 1024 Bit geknackt hat.[74]

5. Insecure Renegotiation wird seit 2009 als schwiegender Bug des SSL-Protokoll eingestuft. Tools zum Ausnutzen der Insecure Renegotiation gibt es auch als OpenSource (z.B. dsniff). Ein Angreifer kann Login Credentials stehlen ohne die SSL-Verschlüsselung knacken zu müssen.[75]

6. SHA sollte laut Empfehlung der IETF nicht mehr als Signaturalgorithmus für die Beglaubigung von Zertifikaten verwendet werden. Die CAs haben inzwischen fast alles umgestellt. Bei Webseiten sollte es keine Problem geben, wenn man diesen Digest Algorithmus abschaltet.

7. Eine SSL-verschlüsselte Webseite sollte nur SSL-verschlüsselte Inhalte darstellen. Unverschlüsselte Elemente sollten nicht geladen werden, um die Sicherheit nicht zu kompromittieren. Firefox blockiert unverschlüsselte aktive Inhalte, lässt Bilder aber zu.

8. FIPS-kompatible Cipher sind per Design schwach ausgelegt und in Firefox standardmäßig deaktiviert.

---

[74] https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto

[75] https://www.verbraucher-sicher-online.de/news/fehlerhaftes-design-im-wichtigsten-verschluesselungsprotokoll-fuer-angriffe-nutzbar

Tracking Risiko durch seltsame SSL/TLS Cipherauswahl

Wenn der Browser eine SSL-verschlüsselte Verbindung zu einem Webserver aufbauen will, dann sendet er Liste der unterstützten TLS-Features, Cipher und der nutzbaren elliptischen Kurven für EC-Crypto. Die Reihenfolge und der Inhalt der Listen ist unterschiedlich für verschiedene Browser und Browser Versionen.

- Die aktuelle Alpha-Version von Firefox sendet beispielsweise:

```
<e name='Firefox/53.0' protocol='771' extTypes='21 23 65281 10 11 16 5 18 40 43 1
suites='4865 4867 4866 49195 49199 52393 52392 49196 49200 49171 49172 51 53'
curves='29 23 24 25 256 257' points='AA==' compress='AA=='/>
```

- Google Chrome sendet:

```
<e name='Chrome/57.0.2951.0' protocol='771' greateExt='1' extTypes='65281 0 23 35
13 5 18 16 30032 11 40 45 43 10 21' greaseSuite='1'
suites='4865 4866 4867 49195 49199 49196 49200 52393 52392 52244 52243 49171 4917
156 157 47 53 10' greaseCurves='1' curves='29 23 24' points='AA==' compress='AA==
```

Das sieht etwas kryptisch aus, man kann sich auf verschiedenen Webseite aber auch anzeigen lassen, was es bedeutet.

Wenn man an den SSL-Ciphern rumspielt und schwache Cipher wie 3DES (Firefox 45) oder Cipher mit DH-Schlüsseltausch deaktiviert, kreiert man möglicherweise ein individuelles Erkennungsmerkmal anhand dessen man beim Aufruf einer verschlüsselten Webseite wiedererkennbar ist. Deshalb empfehlen wir keine Manipulationen an den verwendeten Ciphern. Besser ist es, einen aktuellen Firefox bzw. Firefox ESR zu verwenden und es bei den Einstellungen der Entwickler der NSS Crypto Lib zu belassen.

Empfehlungen für SSL/TLS Konfiguration

Zur Verbesserung der Sicherheit kann man unter der Adresse *about:config* folgende Variablen anpassen.

- RC4-Cipher deaktivieren:

```
security.tls.unrestricted_rc4_fallback  = false
```

- Insecure Renegotiation verbieten (PayPal.com, EBay.de u.a. funktionieren dann nicht mehr):

```
security.ssl.require_safe_negotiation           = true
security.ssl.treat_unsafe_negotiation_as_broken  = true
```

- Strenges Certifikate Pinning erwingen (für Add-on Updates):

```
security.cert_pinning.enforcement_level = 2
```

- Mixed Content verbieten (keine unverschlüsselten Inhalte in HTTPS-Webseiten):

```
security.mixed_content.block_display_content = true
security.mixed_content.block_active_content  = true
```

Hinweis: Für Nutzer vom TorBrowserBundle empfehlen wir NICHT, die Einstellungen zur SSL-Verschlüsselung zu verändern, da individuelle Einstellungen beim SSL-Handshake die Anonymität gefährden können.

Probleme mit sicheren SSL-Einstellungen

Einige Webseiten lassen sich mit diesen Einstellungen nicht via HTTPS aufrufen. Man erhält nur eine leere Seite mit einer Fehlermeldung:

```
Fehlercode: ssl_error_no_cypher_overlap
```

Wenn man diesen Fehler erhält, kann man als erstes kann man RC4 Cipher zulassen oder darauf verzichten, die Webseite zu nutzen. In der Regel ist das Problem damit gelöst.

```
Fehlercode: ssl_error_unsafe_negotiation
```

Wenn dieser Fehler auftritt, dann müsste man Insecure Renegotiation zulassen oder darauf verzichten, die Webseite zu nutzen.

Wenn man unsichere SSL-Einstellungen zulassen muss, dann sollte man sich darüber im klaren sein, dass die Verschlüsselung nicht mehr sicher ist (nach dem Stand der zivilen Forschung). Man sollte sich überlegen, welche privaten Daten man dieser schwachen Verschlüsselung anvertrauen will.

4.14 Starke Passwörter nutzen

Jeder kennt das Problem mit den Passwörtern. Es sollen starke Passwörter sein, sie sollen für jede Site unterschiedlich sein und außerdem soll man sich das alles auch noch merken und auf keinen Fall auf einen Zettel unter der Tastatur "speichern".

- Was ist ein starkes Passwort? Diese Frage muss man unter Beachtung des aktuellen Stand der Technik beantworten. Wörterbuchangriffe sind ein alter Hut. Das Passwort darf kein Wort aus dem Duden sein, das ist einfach zu knacken. Für zufällige Kombinationen aus Buchstaben, Zahlen und Sonderzeichen kann man Cloud Computing für Brute Force Angriffe nutzen. Dabei werden alle möglichen Kombinationen durchprobiert. Ein 6-stelliges Passwort zu knacken, kostet 0,16 Euro. Eine 8-stellige Kombination hat man mit 400 Euro wahrscheinlich und mit 850 Euro sicher geknackt. Man sollte mindestens 10...12 Zeichen verwenden. (Stand: 2011)

- Warum sollte man nicht das gleiche Passwort für viele Logins verwenden? Diese Frage beantwortet der Hack von Anonymous gegen HBGary. Den Aktivisten von Anonymous gelang es, Zugang zur User-Datenbank des Content Management Systems der Website zu erlangen. Die Passwörter konnten geknackt werden. Die Passwörter wurden vom Führungspersonal für weiterer Dienste genutzt: E-Mail, Twitter und Linked-In. Die veröffentlichten 60.000 E-Mails waren sehr peinlich für HBGary [76].

Das Add-on **PwdHash**[77] vereinfacht den Umgang mit Passwörtern. Wenn man vor der Eingabe des Passwortes die Taste F2 drückt oder mit einem doppelten @@ beginnt, wird es in einen einen Hash aus dem Master Passwort und der Domain umgerechnet. Das Ergebnis der Berechnung ist eine 10-stellige zufällige Kombination von Buchstaben und Zahlen und wird als Passwort gesendet. Damit ist es möglich, ein merkbares Master-Passwort für alle Sites zu nutzen, bei denen PwdHash funktioniert. Wichtig ist, dass die Domains der Webseiten für die Eingabe und die Änderung der Passwörter identisch sind.

PwdHash schützt auch vor Phishing-Angriffen. Da die Seite des Phishers von einer anderen Domain geliefert wird, als die originale Website, wird ein falscher Hash generiert, der für den Angreifer wertlos ist.

Sollte man unterwegs auf einem Rechner das Add-on nicht installiert haben, ist das Login-Passwort natürlich nicht zu erraten. Auf der Website des Projektes [78] steht der Algorithmus auch als Javascript Applet zur Verfügung. Man kann sein Master Passwort und die Domain eingeben und erhält das generierte Login Passwort. Das kann man mit Copy & Paste in das Passwort Eingabefeld übernehmen.

Passwortspeicher

Passwortspeicher sind kleine Tools, die Username/Passwort Kombinationen und weitere Informationen zu verschiedenen Accounts in einer verschlüsselten Datenbank verwalten. Es gibt mehrere Gründe, die für die Verwendung eines Passwortspeichers sprechen:

- Viele Programme (z.B. Pidgin) speichern Passwörter unverschlüsselt auf der Festplatte, wenn man die Option zur Speicherung der Passwörter nutzt (nicht empfohlen!). Andere Programme bieten keine Möglichkeit zur Speicherung von Passwörtern, fordern aber die Nutzung einer möglichst langen, sicheren Passphrase (z.B LUKS oder Truecrypt).

- Bei vielen Accounts muss man sich neben Username und Passwort weitere Informationen merken wie z.B. die Antwort auf eine Security Frage oder PINs bei Bezahldienstleistern.

- In der Regel enthalten Passwortspeicher eine Passwortgenerator, der wirklich zufällige und starke Passwörter generieren kann.

[76] http://www.heise.de/ct/artikel/Ausgelacht-1195082.html
[77] https://addons.mozilla.org/de/firefox/addon/pwdhash/
[78] https://www.pwdhash.com

- Das Backup wird deutlich vereinfacht. Man muss nur die verschlüsselte Datenbank auf ein externes Backupmedium kopieren.

Mir gefällt *Keypass*[79] (Windows) bzw. *KeepassX* (Linux) sehr gut. Die Bedienung ist übersichtlich. Man kann Einträge gruppieren, komplizierte Passworte können über die Zwischenablage in die Eingabefelder kopiert werden und müssen nicht (fehlerhaft) abgetippt werden. Um kryptoanalytische Angriffe zu erschweren, kann man die Datenbank mehrere 10.000x mit AES256 verschlüsseln.

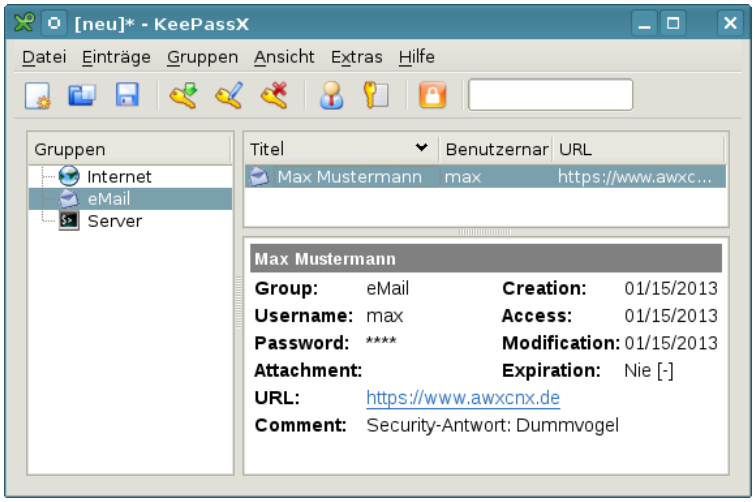


Abbildung 4.21: KeepassX Hauptfenster

Einige Passwortspeicher werben mit der Möglichkeit, die Datenbank zwischen verschiedenen Rechnern und Smartphones zu synchronisieren. Dabei wird die Datenbank *in der Cloud* gespeichert. Das ist für mich ein Graus, vor allem, weil der geheimdienstliche Zugriff auf Daten *in der Cloud* immer mehr vereinfacht wird.

4.15 Zwei-Faktor-Authentifizierung

Einige Webdienste bieten Zwei-Faktor-Authentifizierung (2FA) als Alternative zum einfachen Login mit Username/Passwort an. Die Webseite http://www.dongleauth.info bietet eine Übersicht zu Webdiensten, die OTP oder U2F für den sicheren Login unterstützen.

OTP: Bei der Zwei-Faktor-Authentifizierung mit zusätzlichem One-Time-Passwort besteht das Passwort aus zwei Komponenten, die hintereinander in das Passwortfeld eingegeben werden. Der erste Teil ist üblicherweise ein n-stellige PIN, die man wissen muss. Der zweite Teil ist das One-Time-Passwort. Es wird von einem kleinen Spielzeug

[79] http://keypass.en.softonic.com

geliefert und ist nur einmalig verwendbar.

Wenn ein Angreifer dieses zusammengesetzte Zwei-Faktor-Passwort erbeutet (mit einem Keylogger in einem unsicheren Internet Cafe', durch erfolgreiche Angriffe auf den Datenverkehr), dann ist es wertlos. Außerdem schützt OTP gegen Beobachtung der Passworteingabe durch die ausufernde Videoüberwachung öffentlicher Bereiche und in Internet Cafes.

OTP schützt aber nicht bei Einbrüchen auf dem Server. Da bei OTP der Server und Client den gleichen Algorithmus zur Berechnung und Verifizierung des One-Time-Passworts ausführen, kann ein Angreifer bei erfolgreichem Einbruch die Parameter auslesen und clonen.

Es gibt mehrere Verfahren für die Zwei-Faktor-Authentifizierung:

- **HOTP** (HMAC-based OTP) nutzt One-Time-Passwörter, die aus einem HMAC-SHA1 Hashwert abgeleitet werden, der aus einem Zähler und einem gemeinsam Secret berechnet wurde. Sie sind beliebig lange gültig aber die Verwendung eines Token mit größerem Zählerwert erklärt auch alle Token mit niedrigerem Counter für ungültig.

  Tipp: Wenn man seinen OTP-Generator nicht in den Urlaub o.ä. mitnehmen möchte, kann man sich eine Liste von HOTP-Token generieren lassen und diese Zahlenkombinationen nacheinander zum Login unterwegs verwenden.
- **TOTP** (Time-based OTP) nutzt One-Time-Passwörter, die auf Basis der aktuellen Uhrzeit berechnet werden und nur innerhalb einer kurze Zeitspanne einmalig verwendet werden können.

  Die HOTP oder TOTP Passwörter können von einem Hardware Token (z.B. *Nitrokey Pro* mit der Nitrokey-App) generiert werden oder mit einer Smartphone App (z.B. *FreeOTP* oder *Google Authenticator*). Wenn ein Smartphone genutzt wird muss man die angezeigte Zahlenkombination per Hand in das Login Formular abtippen. Bei der Verwendung von TOTP hat man dafür 30sec bzw. 60 sec Zeit, je nach Konfiguration.

  Wenn man HOTP oder TOTP Login bei einem Webdienst aktiviert, dann wird ein ORCode angezeigt, den man mit dem Smartphone scannt. Mit diesem Scan ist FreeOTP auf dem Smartphone für den Webdienst konfiguriert.
- **YubicoOTP:** ist ein properitäres Protokoll der Firma Yubico. Es wird ein USB-Stick genutzt, der sich wie eine Tastatur verhält. Man aktiviert das Passwortfeld und drückt dann eine Taste auf dem USB-Stick. Damit wird das One-Time-Passwort in das Eingabefeld geschrieben und man kann das Formular abschicken. Neben dem einfachen Yubico Stick gibt es den Yubico NEO, der auch als OpenPGP

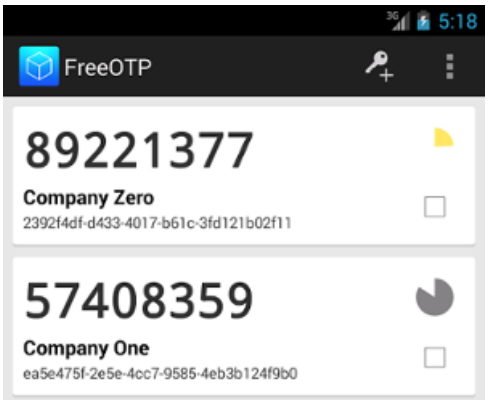


Abbildung 4.22: FreeOTP auf einem Smartphone

Smartcard genutzt werden kann und ab der Version 4 auch als U2F SecurityStick.

U2F: ist ein kryptografisches Privat/Public Key Verfahren zur Authentifizierung mit einem kleinen SecurityStick (z.B. *Nitrokey U2F*[80] oder verschiedene *Yubikeys*[81]), dass im Okt. 2014 standardisiert wurde. Im Gegensatz zu OTP schützt U2F auch bei Einbrüchen auf dem Server und bei der Eingabe des Passwortes auf Phishingseiten.

Das Verfahren läuft im Hintergrund automatisch ab, man muss nur den SecurityStick vor dem Login anschließen. Der Server sendet ein zufälliges Challenge an den Client (Browser), der Browser gibt diesen Input zusammen mit der URL an den SecurityStick weiter, der mit einem geheimen Schlüssel eine Signatur über diese Daten berechnet. Diese Signatur wird als Response an den Server zurück gesendet und kann dort mit dem passenden public Key verifiziert werden.

U2F muss vom Browser und vom Webdienst unterstützt werden. Bisher bietet nur Google Chrome nativen Support für U2F. Mozilla arbeitet an einer Implementierung für Firefox. Bisher gibt es für Firefox das *U2F Support Add-on*[82], das den Browser mit U2F-Support aufmotzt.

SMS: SMS-basierte Verfahren zur Authentifizierung gelten als nicht mehr sicher. Es gibt mehrere Publikationen zu dem Theme. Das NIST empfiehlt, SMS nicht mehr zur Authentifizierung zu nutzen.[83]

> *Out of band verification using SMS is deprecated, and will no longer be allowed in future releases of this guidance.*

ePerso: In Auswertung des US-Wahlkampfes 2016 und dem erheblichen Einfluss von gehackten E-Mail Accounts auf das Wahlverhalten der

[80] https://www.nitrokey.com/de
[81] https://www.yubico.com/products/yubikey-hardware/
[82] https://addons.mozilla.org/de/firefox/addon/u2f-support-add-on
[83] https://pages.nist.gov/800-63-3/sp800-63b.html

amerikanischen Bevölkerung hat die Bundesregierung die Cyber-Sicherheitsstrategien überarbeitet. Nach Ansicht der Bunderegierung ist die Sicherheit mit dem klassischen Benutzername/Passwort-Verfahren nicht mehr gegeben. Im Rahmen Cyber-Sicherheitsstrategien will die Regierung die Bürger stärker zur Nutzung der Onlineausweisfunktion des Personalausweises animieren.

Bezüglich des klassischen Benutzername/Passwort-Verfahren stimmen wir mit der Bundesregierung überein. Wir empfehlen aber die Onlineausweisfunktion des ePerso nicht. Statt dessen sollte man Hardware Token nutzen, die nicht an eine ID-Karte gebunden und vollständig durch den Nutzer konfigurierbar sind.

4.16 Installierte Schriftarten verstecken

Informationen über installierte Schriftarten können mit Javascript, Flash oder Java ausgelesen und zur Berechnung eines individuellen Fingerprint des Browsers genutzt werden. Viele Trackingdienste nutzen inzwischen diese Technik. Die Studie *Dusting the web for fingerprinters*[84] der KU Leuven (2013) kommt zu den Schluss, dass mindestens 0,5 - 1,0% der Webseiten die installierten Schriftarten für Trackingzwecke auslesen.

Viele Webdesigner nutzen Schriften vom Google Font Service. Für den Designer ist die Einbindung der Fonts einfach.

1. Der Webdesigner muss nur ein kleines CSS-Stylesheet importieren. Um die Schriftart OpenSans zu nutzen, reicht z.B. folgende Zeile:

```
<link href='https://fonts.googleapis.com/css?family=Open+Sans'
      rel='stylesheet' type='text/css'>
```

2. Beim Aufruf der Webseite lädt der Browser das Stylesheet vom Server *fonts.googleapis.com*, das Links zum Download der Font Dateien enthält.

3. Der Browser holt sich dann die Dateien mit Schriftarten vom Server *fonts.gstatic.com* und zeigt die Webseite an. Die Font Dateien werden für einen Tag im Cache gespeichert.

Für das Laden von Schriftarten vom Google Font Service gelten die Datenschutzbestimmung von Google[85]. Viele Webseiten weisen in Ihren Privacy Statements aber nicht darauf hin, dass beim Aufruf der Webseite Daten bei Google gespeichert und verarbeitet werden. Wenn man ein Smartphone nutzt, werden bei Google z.B. die Telefonnummer und andere eindeutige Geräte-IDs mit dem Aufruf der Webseite verknüpft.

Das Laden von Schriftarten aus dem Internet ist außerdem ein Sicherheitsrisiko, weil damit Angriffe direkt auf das Betriebssystem möglich werden.

[84] http://www.cosic.esat.kuleuven.be/publications/article-2334.pdf
[85] https://www.google.com/intl/de/policies/privacy

Bugs in den Font Rendering Bibliotheken, die Remote Code Execution durch Laden von bösartigen Schriften erlaubten, gab es für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462).

Firefox Konfiguration

Um das Laden von externen Schriftarten zu blockieren, deaktiviert man in den Einstellungen die Optionen *Webseiten das verwenden von eigenen Schriften erlauben* und die CSS Font Loading API. Damit sehen einige Webseiten nicht mehr ganz so hübsch aus, die Einschränkungen sind aber gering:

```
browser.display.use_document_fonts    = false
layout.css.font-loading-api.enabled   = false
```

Das Underline Handling von Fonts sollte man deaktivieren, da es zum Fingerprinting der installierten Schriftarten und zur Erkennung des Betriebssystems verwendet werden kann:

```
font.blacklist.underline_offset = "" (leerer String)
```

Immer mehr Websites verwenden Webicon Fonts für die Darstellung von Symbolen. Häufig sieht man statt der Symbole seltsame Zeichen, weil der passende Font mit den Symbolen nicht mehr aus dem Internet geladen wird. Das Web wird damit nahezu unbenutzbar.

Um diese Probleme zu vermeiden, empfehlen wir die Freigabe von downloadbaren Schriften für die Darstellung von Symbolen. Das Caching kann man deaktivieren, damit diese Schriften nicht zum Tracking verwendet werden können. Aus Sicherheitsgründen sollte man das Rendering von OpenType SVG Fonts deaktivieren.

```
gfx.downloadable_fonts.enabled            = true
gfx.downloadable_fonts.disable_cache      = false
gfx.font_rendering.opentype_svg.enabled   = false
```

Damit werden Icons wieder korrekt dargestellt:

Um die Lesbarkeit von Webseiten zu verbessern, sollten man gut lesbare Standardschriften verwenden. Unter Windows eignet sich *Arial*, unter Linux eignet sich *Liberation Sans*. Man findet die Option in den Firefox *Einstellungen* auf dem Reiter *Inhalt*. Klicken Sie auf den Button *Erweitert*, um im folgenden Dialog die gewünschten Standardschriftarten zu wählen.

4.17 HTML5 Canvas Elemente

Das HTML5 Canvas Element ist ein Grafikbereich auf der Webseite, in den der Browser mit Javascript zeichnen kann. Ähnlich wie bei einem Zeichenprogramm kann man auch Text schreiben. Die Trackingbranche hat Methoden

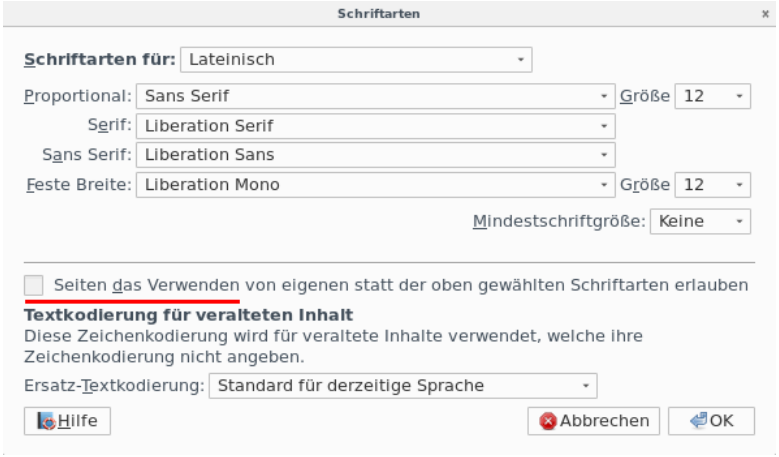


Abbildung 4.23: Schriftarten auswählen

entwickelt, um diese Technologie für die Berechnung eines individuellen Fingerprinting des Browser zu nutzen.

1. Mit Javascript kann ein Text in das Canvas Element geschrieben werden. Danach wird das Ergebnis als Grafik ausgelesen und ein Hashwert von der Grafik berechnet. Das Ergebnis unterscheidet sich von Browser zu Browser aufgrund installierter Schriften, Software für das Rendering usw. Diese Verfahren wurde 2012 in dem Paper *Perfect Pixel*[86] beschrieben und 2016 auf 14.371 Webseiten als Trackingverfahren nachgewiesen.

   Der Canvastest auf Browsewrleaks.com[87] demonstriert das Verfahren und kann Schlussfolgerungen über den verwendeten Browser und das Betriebssystem ableiten (und damit einen User-Agent Fake enttarnen).

   Your Fingerprint :

Signature	1CC7FA60
Found in DB	✔ True
General Conclusion	**It is very likely that you are using [Firefox] on [Ubuntu]**

2. Canvas Font Fingerprinting wurde 2016 in dem *OpenWPM Paper* beschrieben. Dabei wird die Methode *measureText* des *CanvasRenderingContext2D* Objektes genutzt. Der Text wird nicht in das Canvas Element geschrieben sondern es wird nur die Größe ermittelt, die ein Text mit unterschiedlichen Schriftarten benötigen würde, wenn er geschrieben werden würde. Damit ist es möglich, die installierten Schriftarten zu ermitteln, die ein gut geeignetes Merkmal für das Fingerprinting sind.

[86] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf
[87] http://www.browserleaks.com/canvas

Canvas Font Fingerprinting wird bisher nur von einen Trackingdienst genutzt und ist auf 2,5% der TOP1000 Webseiten im Einsatz. Es wird durch Werbeblocker blockiert.

Das Add-on **CanvasBlocker**[88] kann Zugriffe auf HTML5 Canvas Elemente blockieren. Da nur das Auslesen des Canvas als Bild für das Fingerprinting relevant ist, reicht es aus, in des Einstellungen des Add-on nur die Auslese-API zu blockieren oder bei Zugriff auf die Auslese-API um Erlaubnis zu fragen. Dann können Webseiten HTML5 Canvas Elemente zur Gestaltung der Webseite nutzen aber die Ergebnisse des Rendering nicht mehr auslesen.

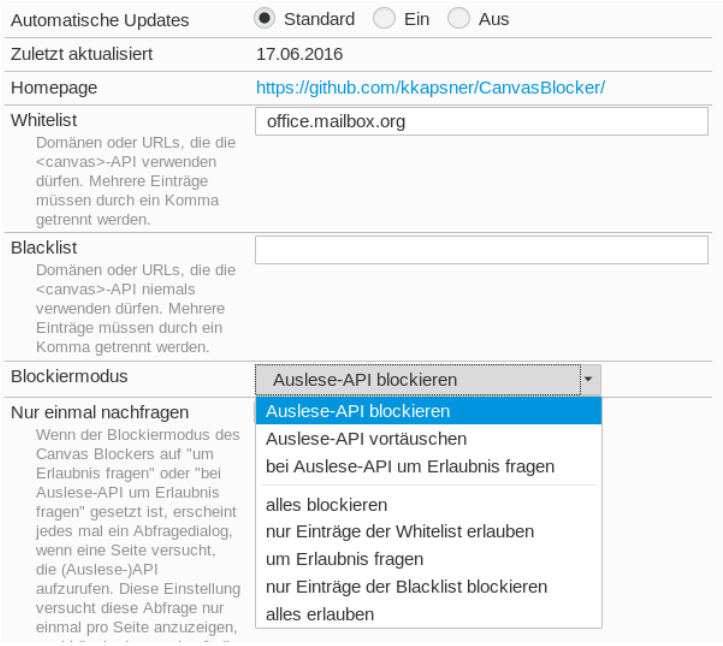


Abbildung 4.24: Konfiguration des Add-on CanvasBlocker

Außerdem kann man eine Whitelist von vertrauenwürdigen Domains bzw. URLs zw definieren, denen der Zugriff auf die gesperrten API Funktionen gestattet wird.

4.18 recource:// URIs blockieren

Via *recource://* URIs kann eine Webseite auf lokale Resource Dateien auf der Festplatte zugreifen und viele Informationen zum Fingerprinting des Browsers auslesen. Es kann das reale Betriebssystem und die Browser Version ermittelt werden, es können Informationen über installierte Add-ons ausgelesen werden (z.B. die Listen von AdBlockern) usw. Der Firefox Test von Browserleaks demonstriert eine kleine Auswahl an Möglichkeiten.[89]

[88] https://addons.mozilla.org/de/firefox/addon/canvasblocker/
[89] https://www.browserleaks.com/firefox

Das Problem ist seit mehr als 3 Jahren bekannt und im Mozilla Bugtracker unter *#863246* und *#903959* beschrieben, im TorBrowser Bugtracker ist das Problem unter *#8725* bekannt.

Das Add-on **No Resource URI Leak**[90] verhindert den Zugriff auf *recource://* ind *chrome://* Adressen für Websites und verhindert damit das Auslesen von Informationen für das Fingerprinting des Browsers.

Die Konfiguration des Add-on kann man mit einem Klick auf den Button *Einstellungen* in der Add-on Verwaltung anpassen (siehe Bild 4.25). Wir empfehlen, den Zugriff auf *recource://* und *chrome://* Adressen zu blockieren sowie den Filter für Redirekts zu aktivieren.

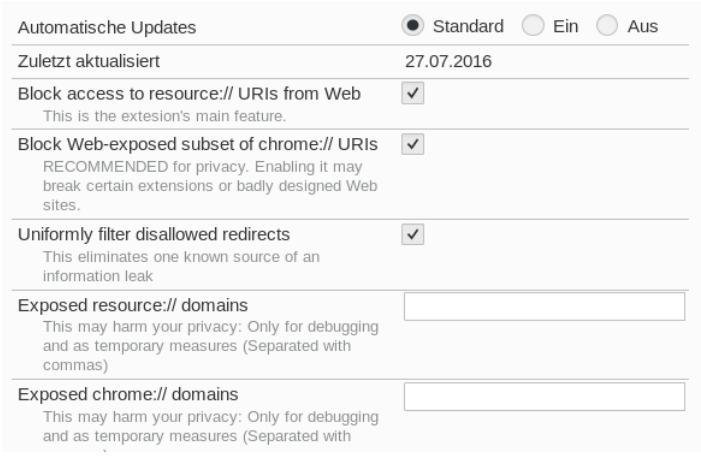


Abbildung 4.25: Konfiguration des Add-on No-Resource-Leak

4.19 User-Agent modifizieren für Firefox

Es ist nicht so einfach, die User-Agent Kennung eines Browsers plausibel zu faken. Eine unsachgemäße bzw. amateurhafte Änderung kann zu einer einzigartigen Kennung führen, die das Tracking enorm erleichtert.

Man kann für einen Firefox nur eine andere Firefox-Kennung verwenden. Die verschiedenen Browser sind durch individuelle Headerzeilen und -reihenfolge im HTTP-Request beim Aufruf einer Webseite unterscheidbar. Eine Tarnung mit dem User-Agent eines anderen Browsers ist leicht als Fake zu identifizieren und sehr leicht zu verfolgen. Viele Add-ons zum Spoofen der User Agent Kennung machen diesen Fehler, wie der Anonymitätstest von JonDonym zeigt.

[90] https://addons.mozilla.org/de/firefox/addon/no-resource-uri-leak

- Das Add-on *User-Agent-Overrider* (Version 0.2.5.1) sollte im Test einen Internet Explorer 9.0 für Win64 faken. Die Header Signatur entlarvt den Browser jedoch als einen Firefox, der sich als IE tarnen will.

Signatur	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

- Das Add-on *Random-Agent-Spoofer* (Version 0.9.5.2) sollte im Test einen Google Chrome Browser 41.0 für Win64 faken. Die Header Signatur entlarvt den Browser ebenfalls als Firefox, der sich tarnen will.

Signatur	8ab3a24c55ad99f4e3a6e5c03cad9446 (Firefox)
User-Agent	Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36

Schlussfolgerung: Lasst die Finger von diesen und ähnlichen Add-ons.

Einige Firefox Versionen unterscheiden sich nicht nur im User-Agent, sondern auch sehr subtil in einigen anderen HTTP-Headern. Man beachte das Leerzeichen nach dem Komma bei Firefox 10:

```
ACCEPT-ENCODING "gzip,deflate"      (Firefox 3.6.x)
ACCEPT-ENCODING "gzip, deflate"     (Firefox 10.0.x)
```

Außerdem unterscheidet sich die Release Version von Firefox in den Features von der ESR-Version (Extended Support Release). Die Unterschiede werden größer, je weiter sich die Release Version von der ESR-Version entfernt.

Die Browser der Anonymisierungsdienste faken auch die Sprache des Browsers, um eine möglichst große Anonymitätsgruppe zu bilden. Für das Surfen ohne IP-Anonymisierung emfehlen wir diese Fakes aus folgenden Gründen nicht:

1. Es ist einfach plausibler, wenn man mit einer deutschen IP-Adresse beim Besuch einer deutschsprachigen Webseite auch einen deutschen Browser verwendet.

2. Mit Hilfe der *JavaScript Localisation API* können diese Fakes bei aktivem Javascript entlarvt werden, wenn man keine zusätzlichen Schutzmaßnahmen wie beim TorBrowser implementiert. Mit der Javascript Funktion *toLocaleString()* kann man beispielsweise Datums- und Zeitangaben in die bevorzuge Desktop(!) Lokalisierung des Nutzers umrechnen lassen und das Ergebnis auswerten:

   ```
   ACCEPT-ENCODING "gzip,deflate"      (Firefox 3.6.x)
   ACCEPT-ENCODING "gzip, deflate"     (Firefox 10.0.x)
   ```

3. Durch Auswertung der Keyboard Events könnte ein Angreifer die Lokalisierung der Tastatur ermitteln. Die Verwendung eines deutschen Browsers ist in Kombination mit einer deutschen Tastatur ebenfalls plausibler. Die Keyboard Events können unter *about:config* deaktiviert werden (siehe: Hardware Fingerprinting).

Wenn man einen englischen Browser (en-US) haben möchte, dann sollte man einen englischen Browser installieren und den Desktop auf Englisch umschalten.

Der Browser hängt in viele Dingen von Bibliotheken des Betriebssystems ab. Durch Auswertung einige Seltsamkeiten lässt sich das real verwendete Betriebssystem teilweise identifizieren oder zumindest ein User-Agent Fake als Fake entlarven. Ein Beispiel OS-spezifische Seltsamkeiten ist das Ergebnis der folgenden Javascript Berechnung:

```
Math.tan(-1e300) = -4.987183803371025  (Windows)
Math.tan(-1e300) = -1.4214488238747245 (Linux, iOS)
```

Plug-ins verraten in der Regel das verwendete Betriebssystem und können keinen Fake konfigurieren. Wenn man auf Flash u.ä. nicht verzichten kann, dann sollte man keinen User-Agent Fake verwenden. Ein Linux Nutzer mit einem Windows Firefox Fake ist leicht anhand des Browser Fingerprint identifizierbar und verfolgbar, wenn der Flash-Player die Information liefert, dass er eigentlich Linux 64Bit verwendet.

Schlussfolgerung

Es ist nahezu unmöglich, die User-Agent Kennung des Browsers plausibel zu faken. Ein unvollständiger Fake-Versuch ist aber ein gutes Identifizierungsmerkmal für Trackingdienste. Man könnte einen häufig verwendten Browser verwenden. Das ist die einzige Empfehlung, die wir zu dem Thema geben können.

4.20 Hardware Fingerprinting

Über verschiedenen API-Schnittstellen können Trackingscripte Informationen über die Hardware des Rechners sammeln. Durch Messung der Performance aufwendiger Grafik Rendering Operationen oder beim Abspielen von Videos können Trackingscripte ebenfalls Informationen über die Hardware sammeln.

Bildschirm: Informationen über die Größe des Monitors und des Browserfensters werden am häufigsten für das Hardwarefingerprinting genutzt. Es liegen keine wissenschaftlichen Analysen zur Verbreitung dieser Trackingmethode vor, aber grob geschätzt werden diese Informationen von 30-50% der Webseiten ausgewertet. Insbesondere auf größeren Portalen wie heise.de, spiegel.de, zeit.de oder google.com findet man fast immer Trackingscripte, die Bildschirmgröße und Größe des Browserfensters für das Fingerprinting des Browsers nutzen.

Das Auslesen der Bildschirmgröße kann man verhindern, indem folgende Variable unter *about:config* neu angelegt wird:

```
privacy.resistFingerprinting = true
```

Wenn diese Variable gesetzt wurde, dann wird wie beim TorBrowser die Fenstergröße des Browser gleichzeitig als Bildschirmgröße verwendet und die reale Größe des Bildschrims ist nicht auslesbar. Derzeit ist die Firefox Implementierung nicht kompatibel mit dem ClearClick Schutz von NoScript und liefert viele falsche Alarme. Deshalb empfehlen wir diese Einstellung noch nicht sondern die Deaktivierung von Javascript.

Batterie-API: Aus unbekannten Gründen ist im HTML5-Standard eine API für den Zugriff auf den Status des Laptop Akku vorgesehen. Damit ist es möglich, den Ladezustand des Akku sowie den Status des Stromanschluss abzufragen. Um zu verhindern, dass der Ladezustand der Batterie oder dass das Vorhandensein eines Akku für das Hardware Fingerprinting genutzt wird, sollte man die API unter *about:config* deaktivieren:

```
dom.battery.enabled = false
```

Auch Mozilla hat inzwischen eingesehen, dass dieses Feature technisch sinnlos ist und nur für Tracking genutzt. Es wird in Firefox 52 entfernt.

Gamepad-API: Die Gamepad-API liefert Informationen über einen angeschlossenen Gamepad. Das ist ein überwiegend sinnloses Feature und kann ebenfalls unter *about:config* deaktiviert werden:

```
dom.gamepad.enabled = false
```

Keyboard-API: Erste Funktionen der Keyboard-API wurden in Firefox 38.0 standardmäßig aktiviert. Durch Auswertung der Keyboard Events beim Schreiben in Formularen kann ein Trackingscript z.B. ermitteln, ob eine deutsche oder englische Tastatur verwendet wird. Die Keyboard Events können unter *about:config* deaktiviert werden:

```
dom.keyboardevent.code.enabled                = false
dom.beforeAfterKeyboardEvent.enabled          = false
dom.keyboardevent.dispatch_during_composition = false
```

MediaDevices: In Firefox 39 wurde die Funktion zum Auslesen der Media Input und Output Devices[91] standardmäßig aktiviert. Damit können Informationen über Kamera, Mikrophone oder Sound Ausgabe für das Hardware Fingerprinting genutzt werden. Diese API kann mit folgender Option deaktiveirt werden:

```
media.navigator.enabled = false
```

Grafikhardware: Die Hardwarebeschleunigung des Rendering kann man deaktivieren, um ein Fingerprinting der Grafikhardware zu verhindern. Die Einbußen sind kaum erkennbar.

```
gfx.direct2d.disabled                  = true
layers.acceleration.disabled           = true
media.hardware-video-decoding.enabled  = false
```

[91] https://developer.mozilla.org/en-US/docs/Web/API/MediaDevices/enumerateDevices

Statistiken für Videos: Die Übermittlung von Statistiken beim Abspielen von Videos (Framerate usw.) kann unter *about:config* deaktiviert werden:

```
media.video_stats.enabled = false
```

Face Detection: Die Camera-API von Firefox kann Gesichter erkennen (nur Face Detection, nicht Face Recogbition) und mit dem Tracking Focus einem Gesicht folgen. Die Technik ist nicht privacy invasive, man braucht es aber auch nicht, um Webseiten zu betrachten. Unter *about:config* kann man diese Features deaktivieren: man die API unter *about:config* deaktivieren:

```
camera.control.face_detection.enabled            = false
camera.control.autofocus_moving_callback.enabled  = false
```

4.21 Sonstige Maßnahmen

Am Schluss der Konfiguration gibt es noch ein paar kleine Maßnahmen, die überflüssige Features im Browser deaktivieren, die Informationen preisgeben.

Geolocation-API deaktivieren

Mit Hilfe der Geolocation-API kann die geografische Position des Surfer relativ genau bestimmt werden. Zur Ortsbestimmung können je nach vorhandener Hardware im Rechner die WLANs in der Umgebung genutzt werden, GPS-Hardware oder ... Im ungünstigsten Fall kann der Standort nur anhand der IP-Adresse bestimmt werden. Aktuelle Firefox Versionen fragen nach, bevor der Zugriff auf die Geolocation API erlaubt wird. Trotzdem habe ich ein besseres Gefühl, wenn man es komplett deaktiviert. Dafür muss man unter *about:config* die folgende Variable setzen:

```
geo.enabled = false
geo.wifi.uri = "" (leerer String)
```

Diese Einstellung ist wichtig, wenn man die eigene IP-Adresse mit VPNs oder Anonymisierungsdiensten versteckt.

WebGL deaktivieren

WebGL stellt eine Javascript-API für das Rendering von 3D-Objekten bereit. Es kann für das Fingerprinting der Performance der Grafikhardware und OpenGL Implementierung genutzt werden, wie die Studie *Perfect Pixel: Fingerprinting Canvas in HTML5* [92] zeigt. Das Fingerprinting via WebGL kann mit folgenden Einstellungen verhindert werden:

```
webgl.disable-extensions                      = true
webgl.min_capability_mode                     = true
webgl.disable-fail-if-major-performance-caveat = true
```

[92] http://www.w2spconf.com/2012/papers/w2sp12-final4.pdf

Außerdem ist WebGL ein (unnötiges) Sicherheitsrisiko, weil damit Angriffe auf das Betriebssystem möglich werden. Durch nachgeladene Schriften können Bugs in den Font Rendering Bibliotheken ausgenutzt werden, das gab es für Windows (ms11-087), Linux (CVE-2010-3855) oder OpenBSD (CVE-2013-6462). Die WebGL Shader Engines haben auch gelegentlich Bugs, wie z.B. MFSA 2016-53. Deshalb empfehlen wir, WebGL komplett zu deaktivieren, um das Risiko zu reduzieren:

```
webgl.disabled = true
```

WebRTC deaktivieren

WebRTC ist eine Technologie, die direkte Telefonie ud Videochats zwischen Surfern im Browser ermöglichen soll. Derzeit gibt es wenig sinnvolle Anwendungen für diese Technologie und ich würde ein spezialisiertes Programm wie Jitsi bevorzugen. Wer es einmal ausprobieren möchte, kann sich https://palava.tv oder http://browsermeeting.com anschauen.

Mit WebRTC kann die lokale IP Adresse des Rechners im LAN und die öffentliche IP Adresse ermittelt werden. Bei IPv4 Adressen ist es in der Regel nicht öffentliche IP-Adresse sondern die Adresse im internen LAN, trotzdem ist es ein Identifikationsmerkmal. Bei Firefox kann man WebRTC unter *about:config* deaktivieren:

```
media.peerconnection.enabled = false
loop.enabled                 = false
```

Timing APIs deaktivieren

Die hochgenauen Timing APIs können von Webanwendungen zur Analyse des Ladens von Resourcen oder des Nutzerverhaltens missbraucht werde, siehe: *Timing Attacks on Web Privacy*[93]. Wenn man seinen Browser zum Lesen von Webseiten und nicht vorrangig für Games verwendet, sollte man die APIs deaktivieren:

```
dom.enable_resource_timing = false
dom.enable_user_timing     = false
dom.enable_performance     = false
```

Clipboard Events deaktivieren

Mit den Clipboard Events informiert Firefox eine Webseite, dass der Surfer einen Ausschnitt in die Zwischenablage kopiert hat oder den Inhalt der Zwischenablage in ein Formularfeld eingefügt hat. Es werden die Events *oncopy, oncut* and *onpaste* ausgelöst, auf die die Webseite irgendwie reagieren könnte. Man kann diese Events unter *about:config* deaktivieren:

```
dom.event.clipboardevents.enabled = false
```

[93] http://sip.cs.princeton.edu/pub/webtiming.pdf

Außer bei Google Docs und ähnliche Javascript-lastigen GUIs zur Dokumentenbearbeitung in der Cloud ist mir keine sinnvolle Anwendung dieses Features bekannt.

Spekulatives Laden von Webseiten

Firefox beginnt in einigen Situationen bereits mit dem Laden von Webseiten, wenn sich der Mauszeiger über einem Link befindet, also bevor man wirklich klickt. Damit soll das Laden von Webseiten einige Millisekunden beschleunigt werden. Wenn man Verbindungen mit unerwünschten Webservern vermeiden möchte, kann man das Feature unter *about:config* abschalten:

```
network.http.speculative-parallel-limit = 0
```

WebIDE deaktivieren

TorProject.org empfiehlt für Firefox 38.0 ff. aus Sicherheitsgründen, die WebIDE unter *about:config* zu deaktivieren:

```
devtools.webide.enabled = false
devtools.webide.autoinstallADBHelper = false
devtools.webide.autoinstallFxdtAdapters = false
```

Kill Switch für Add-ons abschalten

Die Extension blocklist[94] kann Mozilla nutzen, um einzelne Add-ons im Browser zu deaktivieren. Es ist praktisch ein kill switch für Firefox Add-ons und Plug-ins. Beim Aktualisieren der Blockliste werden detaillierte Informationen zum realen Browser und Betriebssystem an Mozilla übertragen.

```
https://addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a
-464f-9b0e-13a3a9e97384%7D/10.0.5/Firefox/20120608001639
/Linux_x86-gcc3/en-US/default/Linux%202.6.37.6-smp%20
(GTK%202.24.4)/default/default/20/20/3/
```

Ich mag es nicht, wenn jemand remote irgendetwas auf meinem Rechner deaktiviert oder deaktivieren könnte. Unter *about:config* kann man dieses Feature abschalten:

```
extensions.blocklist.enabled = false
```

Update der Metadaten für Add-ons deaktivieren

Seit Firefox 4.0 kontaktiert der Browser täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons und die Zeit, die Firefox zum Start braucht. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhägig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. Unter *about:config* kann man diese Funktion abschalten:

```
extensions.getAddons.cache.enabled = false
```

[94] https://addons.mozilla.org/en-US/firefox/blocked

Download der Safebrowsing Datenbank deaktivieren

Ab Firefox 34.0 reicht es nicht mehr, die Nutzung von Googles Safebrowsing Datenbank im Einstellungsdialog zu deaktivieren. Zusätzlich muss man den Download der Datenbank unter *about:config* abschalten, wenn man keine Verbindungen zu Google herstellen will:

```
browser.safebrowsing.enabled                    = false (bis Firefox 49)
browser.safebrowsing.phishing.enabled           = false (ab Firefox 50)
browser.safebrowsing.malware.enabled            = false
browser.safebrowsing.blockedURIs.enabled        = false
browser.safebrowsing.downloads.enabled          = false
browser.safebrowsing.downloads.remote.enabled   = false
```

Healthreport deaktivieren

Der Healthreport wird an Mozilla gesendet, kann man unter *about:config* deaktivieren:

```
datareporting.healthreport.service.enabled = false
datareporting.healthreport.uploadEnabled   = false
datareporting.policy.dataSubmissionEnabled = false
```

Heartbeat User Rating deaktivieren

Mit Firefox 37.0 hat Mozilla das heartbeat user rating system eingeführt. Der User soll Firefox bewerten und wird gelegentlich zur Teilnahme an der Community eingeladen. Mozilla hat selbst erkannt, dass dieses Feature nerven könnte:

> *We understand that any interruption of your time on the internet can be annoying.*

Unter *about:config* kann man das Feature deaktivieren, indem man die folgende URL auf einen leeren String setzt:

```
browser.selfsupport.url =
```

Wi-Fi Hotspot Portalerkennung deaktivieren

Firefox 52 erkennt die Portalseiten von Wi-Fi Hotspots und öffnet sie in einem neuen Tab (Release Notes). Für die Wi-Fi Hotspot Portalerkennung kontaktiert Firefox bei jedem(!) Start folgende Webseite:

```
http://detectportal.firefox.com/success.txt
```

Unter *about:config* kann man Firefox dieses Verhalten abgewöhnen, indem man die Portalerkennung deaktiviert (man wird es kaum vermissen):

```
network.captive-portal-service.enabled = false
```

4.22 Snakeoil für Firefox (überflüssiges)

Auf der Mozilla-Website für Add-ons findet man tausende von Erweiterungen. Man kann nicht alle vorstellen. Ich bekomme immer wieder Hinweise auf dieses oder jenes privacyfreundliche Add-on und habe ein paar Dinge zusammengestellt, die ich nicht in die Empfehlungen aufnehme.

Als Grundsicherung empfehlen wir die Kombination von *CookieController* + *NoScript* + *uBlock Origin* (o.ä) + *HTTPSEverywhere* + *CanvasBlocker* und evtl. *RefControl*. Viele Add-ons bieten Funktionen, die von dieser Kombination bereits abgedeckt werden. Andere sind einfach nur überflüssig.

PrivacyBadger der EFF.org

Das Add-on lernt anhand der Verteilung der Cookies beim Surfen selbständig, welche Domains das Surfverhalten tracken. Das ist ein interessantes Konzept. Wir teilen aber die Vorbehalte von TorProject.org gegen dieses Konzept.

- Es entstehen dabei individuelle Blocklisten, die für das Fingerprinting genutzt werden können. Es ist bekannt, dass man Seiteneffekte von Add-ons (NoScript Whitelist, AdBlock Filterlisten) für das Fingerprinting des Browsers nutzen kann. PrivacyBadger liefert einen dynamischen, aber sehr individuellen Fingerprint.

- Es werden Informationen über das Surfverhalten auf der Festplatte gespeichert (unerwünscht) und außerdem werden durch die individuelle Blockliste indirekt Informationen über die Surf-History an die Webseiten geliefert.

Web of Trust (WOT)

WOT ist ein Add-on, das den Surfer über die Reputation der besuchten Webseite informiert. Das Add-on wird häufig empfohlen. Während des Surfens sammelt WOT Daten über den Besuch jeder Webseite und überträgt die Daten an die Betreiber des Dienstes. Die Daten werden mit schwacher Anonymisierung zu Profilen verknüpft und auch an die Werbeindustrie verkauft, wie Reporter des NDR zeigten. Die Daten konnten relativ einfach deanonymisiert werden und lieferten umfangreiche Informationen zu Krankheiten, sexuelle Vorlieben und Drogenkonsum einzeln identifizierbarer Personen. Unschön, wenn über einen Richter bekannt wird, dass er eine Vorliebe Sado-Maso Praktiken hat o.ä.

Google Analytics Opt-Out

Das Add-on von Google verhindert die Ausführung der zu Google-Analytics gehörenden Scripte. Die Scripte werden jedoch trotzdem von den Google Servern geladen und man hinterlässt Spuren in den Logdaten. Google erhält die Informationen zur IP-Adresse des Surfers und welche Webseite er gerade besucht (via Referer). Außerdem gibt es über hundert weitere Surftracker, die ignoriert werden.

Die Add-ons *NoScript* zusammen mit einem AdBlocker wie *uBlock Origin* erledigen diese Aufgabe besser.

GoogleSharing

Das Add-on verteilt alle Anfragen an die Google-Suche, Google-Cookies usw. über zentrale Server an zufällig ausgewählte Nutzer von GoogleSharing. Die Ergebnisse werden von den zufällig ausgewählten Nutzern über die zentralen Server zurück an den lokalen Firefox geliefert.

Nach unserer Meinung verbessert man seine Privatsphäre nicht, indem die Daten einem weiteren Dienst zur Verfügung stellt. Das der eigene Rechner dabei auch unkontrolliert Daten von anderen Nutzern stellvertretend an Google weiterleitet, ist ein unnötiges Risiko. Google speichert diese Informationen und gibt sie breitwillig an Behörden und Geheimdienste weiter. So kann man unschuldig in Verwicklungen geraten, die amn lieber vermeiden möchte. Bei daten-speicherung.de findet man aktuelle Zahlen zur Datenweitergabe von Google an Behörden und Geheimdienste:

- 3x täglich an deutsche Stellen
- 20x täglich an US-amerikanische Stellen
- 6x täglich an britische Stellen

Statt GoogleSharing sollte man lieber privacy-freundliche Alternativen nutzen: die Suchmaschine Ixquick.com oder Startingpage.com, für E-Mails einen Provider nutzen, der den Inhalt der Nachrichten nicht indexiert, openstreetmap.org statt Google-Maps verwenden...

Zweite Verteidigungslinie?

Eine Reihe von Add-ons bieten Funktionen, welche durch die oben genannte Kombination bereits abgedeckt werden:

- *FlashBlock* blockiert Flash-Animationen. Das erledigt auch NoScript.
- *ForceHTTPS* kann für bestimmte Webseiten die Nutzung von HTTPS erzwingen, auch diese Funktion bietet NoScript.
- *Targeted Advertising Cookie Opt-Out* und *Ghostery* blockieren Surftracker. Es werden Trackingdienste blockiert, die auch AdBlock Plus oder uBlock Origin mit der *EasyPrivacy Liste* sehr gut blockiert. Außerdem gibt es immer wieder Probleme mit *Ghostery* auf einigen Webseiten, da das Add-on kein Whitelisting kennt.
- *No FB Tracking* blockiert die Facebook Like Buttons. Auch das kann AdBlock Plus besser. Die SocialMediaBlock Liste von MontzA blockieren nicht nur Facebook Like Buttons sondern andere Social Networks.
-

Wer meint, es nutzen zu müssen - Ok.

Kapitel 5

Bezahlen im Netz

Der bekannteste Bezahldienstleister im Internet ist zweifellos **PayPal.com**. Die Firma wurde von Peter Thiel gegründet, der u.a. den Datensammler Rapleaf.com aufgebaut hat, als einer der Hauptinvestoren die Entwicklung von Facebook maßgeblich mitbestimmt hat und zum Steering Committee der Bilderberg Konferenzen gehört. Das Credo von P. Thiel ist eine totale Personalisierung des Internet.

Die Nutzung von PayPal.com ist das Gegenteil von anonym. Bei jedem Zahlungsvorgang wird eine Verknüpfung von persönlichen Daten (E-Mail Adresse, Kontoverbindung) und gekauften Waren hergestellt. Die Daten werden an mehr als 100 Firmen übertragen zum Monitoring der Überweisung.

PayPal.com nutzt seine Marktposition für die Durchsetzung politischer Interessen der USA. Gemäß der Embargo-Politik der USA werden Internetnutzer in über 60 Ländern ausgesperrt. Internationales Aufsehen erregte die Sperrung der Konten von Wikileaks. Daneben gibt es viele weitere Fälle. Mehr als 30 deutschen Online-Händlern wurden die Konten gesperrt [1], weil sie kubanische Produkte (Zigarren, Rum, Aschenbecher) in Deutschland anboten. Die Sperre wurde mit einem amerikanischen Handelsembargo gegen Kuba begründet, das für Europäer belanglos ist.

Aufgrund dieser politischen Instrumentalisierung hat *Anonymous* zum Boykott von PayPal.com aufgerufen und an Nutzer appelliert, ihre Accounts bei diesem Bezahldienst zu kündigen. 35.000 PayPal-Nutzer sollen dem Aufruf umgehend gefolgt sein.

Zukünftig möchte PayPal.com auch in der realen Welt präsent sein. Das Bezahlsystem soll die Geldbörse in zwei Jahren ersetzen, wie Ebay-Chef John Donahoe sagte, natürlich mit den üblichen Schnüffeleien:

> *Beim Einsatz von PayPal in den Geschäften könnten die Einzelhändler mehr über Vorlieben ihrer Kunden erfahren und sie entsprechend besser bedienen.*

[1] http://heise.de/-1320630

5.1 Kreditkarten

Die Kreditkarte ist ein ungeeignetes Zahlungsmittel im Internet. Es ermöglicht das Tracking aller Einkäufe im Web. Außerdem kann die Kreditkarte durch Datenverluste beim Online-Händler kompromittiert werden. Das passiert öfters und in Carder-Foren kann man diese Kreditkarten für 3-10 Euro kaufen.

- 400.000 Kunden beim Internetkonzern Unister betroffen (Dez. 2012).[2]
- 1,5 Millionen Kunden bei Global Payments betroffen (Juni 2012).[3]
- Tausenden Nutzer der israelischen Sport-Webseite One.co.il betroffen (Jan. 2012).[4]
- 24 Millionen Kunden der Amazon-Tochter Zappos betroffen (Jan. 2012).[5]

Auch in Läden kann die Nutzung von Kreditkarten ein Risiko sein. Die größten Raubzüge erfolgten mit gehackten Kartenterminals. Dabei können auch PINs abgegriffen werden:

- Bis zu 40 Mio. Kreditkartendaten bei US-Shoppingriesen Target kopiert, auch PINs wurden abgeschnorchelt.[6]
- US-Handelskette Neiman Marcus räumte ein, dass bei Angriffen auf ihre Computersysteme 1,1 Mio. Kreditkarten abgeschorchelt wurden.

Die Kreditkartenfirma Mastercard demonstriert mit dem Patent 20160358272 (veröffentlicht Dez. 2016), wie man sich die Monetarisierung des angesammelten Datenreichtums der Kreditkartenfirmen zukünftig vorstellen kann. In dem Patent wird beschrieben, wie die Kreditkartenfirmen aus den Einkäufen anhand der Konfektions- und die Schuhgrößen die Größe und das Gewicht des Karteninhabers ermittlen können. Diese Daten könnten an Fluggesellschaften verkauft werden, die damit die Sitzverteilung für die Passagiere optimieren könnten.

(Das ist ein sehr schönes Beispiel für die neuen Produkte, die laut Bundeskanzlerin Merkel aus Datenreichtum generiert werden könnten, wenn wir uns endlich von den überholten Konzepten des vergangenen Jahrhunderts wie Datenschutz und Privatsphäre verabschieden würden.)

Prepaid-Kreditkarten

Eine Alternative sind Prepaid-Kreditkarten. An Tankstellen usw. kann man Prepaid-Karten von *mywirecard.com* kaufen. Die Karte kostet ca. 10 Euro und kann bis zu 100,- Euro mit Bargeld beim Kauf aufgeladen werden. Man zahlt also 10% Security-Bonus.

Die Prepaid-Karte muss anschließend im Internet aktiviert werden. Dabei wird ein Code per SMS an eine Handynummer gesendet, der auf der Internetseite einzugeben ist. Die Anonymität hängt also davon ab, ob man ein

[2] http://www.mdr.de/nachrichten/unister130.html
[3] http://heise.de/-1617091
[4] http://heise.de/-1403584
[5] http://www.golem.de/1201/89081.html
[6] http://heise.de/-2070721

anonymes Prepaid-Handy nutzt. Man braucht nicht immer die große, richtige Anonymität. Wenn ich ein SSL-Zertifikat für den Webserver awxcnx.de kaufe, dann ist mehr oder weniger eindeutig klar, wer dahinter steckt. Vergleichbare Anwendungsbeispiele lassen sich für den Leser sicher leicht finden.

Mit einer Prepaid-Karte kann man einen anonymen PayPal-Account mit fiktiven Daten anlegen. Das eröffnet Möglichkeiten zur anonymen Nutzung von kommerziellen Angeboten im Internet wie Wuala oder Cilent Circle, die nur Bezahlung via PayPal.com oder Kreditkarte anbieten.

Hinweis: Tor Onion Router kann nicht als Anonymisierungsdienst für PayPal.com genutzt werden. Paypal.com prüft anhand der IP-Adresse den Standort des Nutzers und sperrt den Account, wenn etwas seltsames passiert. Wenn man sich bspw. mit einer deutschen IP-Adresse einloggt und 10min später mit einer amrikanischen IP-Adresse auf den Account zugreifen möchte, dann geht PayPal.com von einem Hacker-Angriff aus und sperrt den Account. Mit JonDonym gibt es keine Probleme, wenn man immer die gleiche Mix-Kasakde nutzt.

5.2 Bezahlsysteme der Deutschen Bahn

Am 28. September 2011 veröffentlichte die Leaking Plattform Cryptom.org in der Liste der *Online Spying Guides* einen *Leitfaden zum Datenzugriff* der Generalstaatsanwaltschaft München.

Das Dokument zeigt auch, wie das Bezahlsystem der Deutschen Bahn in die Überwachung eingebunden wird. Für das e-Ticketing der Deutschen Bahn gibt es ein konkretes Überwachungszenario. Durch die Abrechnung übers Mobiltelefon verfüge die Deutsche Bahn über die Daten sämtlicher Funkzellen, die der Nutzer durchfahren hat. Diese Daten werden langfristig gespeichert und können von den Behörden auf Gundlage von §100g StPO abgerufen werden. Der Zugriff auf die Reiseprofile ist damit nicht nur bei schweren Straftaten möglich, sondern auch bei allen Straftaten, die mittels Telekommunikationstechnik begangen wurden.

Das Beispiel zeigt, wie bei Nutzung Handy-basierter Bezahlmethoden neue Datenbestände anhäufen. Teilweise können diese Daten auch als Rechnungsdaten abgerufen werden ohne die juristischen Hürden des Zugriffs auf Kommunikationsdaten.

Als Konsequenz kann man Reisenden mit der Deutschen Bahn nur zu anonymen Bargeldzahlungen raten. Wie schnell man plötzlich ein *Terrorist* wird, zeigte das Beispiel *Andrej Holm*.

5.3 SOFORT Überweisung

SOFORT Überweisung ist ein Online-Zahlungssystem zur bargeldlosen Zahlung im Internet. Bei dem Bezahlvorgang stellt der Kunde dem Zah-

lungsdienstleister Sofort GmbH die notwendigen Credentials für den Online Zugriff (PIN usw.) auf sein Konto zur Verfügung. Die Sofort GmbH nutzt diese Informationen, um sich Daten über Kontostand u.ä zu holen und danach die Transaktion auszuführen.

Würde man das Verfahren in die Offline-Welt übertragen, könnte man die Dienstleistung der SOFORT Überweisung wie folgt beschreiben: Weil man selbst zu faul ist, gibt man einem Fremden auf der Straße die EC-Karte und PIN, damit er zum Bankautomaten geht, sich über den Kontostand und die letzten Transaktionen informiert um danach die gewünschte Überweisung auszuführen.

In den AGBs verbieten es alle Banken und Sparkassen den Kunden, die Credentials für den Online Zugriff Dritten zur Verfügung zu stellen. Mit der Nutzung von SOFORT Überweisung verstößt man also gegen die AGBs der Finanzinstitute.

Das Landgericht Frankfurt am Main hat es in einem Urteil klar formuliert, das die Nutzung des Dienstes unzumutbar ist, egal welche Sicherheitsgarantien von der Sofort GmbH versprochen werden:

> *Die Nutzung des Dienstes Sofortüberweisung ist unabhängig von seiner Bewertung durch Kreditinstitute für den Verbraucher unzumutbar, da er hierzu nicht nur mit einem Dritten in vertragliche Beziehungen treten muss, sondern diesem Dritten auch noch Kontozugangsdaten mitteilen muss und in den Abruf von Kontodaten einwilligen muss. Hierdurch erhält ein Dritter umfassenden Einblick in die Kunden-Kontoinformationen. Hierbei handelt es sich um besonders sensible Finanzdaten, die auch zur Erstellung von Persönlichkeitsprofilen genutzt werden könnten. Daneben muss der Kunde dem Zahlungsdienstleister seine personalisierten Sicherheitsmerkmale (zum Beispiel PIN und TAN) mitteilen. Dies birgt erhebliche Risiken für die Datensicherheit und eröffnet erhebliche Missbrauchsmöglichkeiten. Dabei kommt es im Ergebnis nicht auf die konkrete Sicherheit des Dienstes Sofortüberweisung an, sondern auf die grundsätzliche Erwägung, dass der Verbraucher nicht gezwungen werden kann, seine Daten diesem erhöhten Risiko auszusetzen.*

5.4 Paysafecard, UKash, Pecunix

Bei der Nutzung von Alternativen ist man abhängig von den Angeboten der Online-Händler. Man kann nicht bei allen Händlern mit allen Varianten bezahlen und muss als Kunde etwas flexibel sein.

- **Paysafecard:** entstand aus einem Forschungsprojekt der EU. In vielen Geschäften oder Tankstellen kann man Gutscheincodes kaufen. Die Webseite von Paysafecard bietet eine Umkreis-Suche nach Verkaufstellen. Diese Codes kann man ähnlich anonym wie Bargeld im Web zur Bezahlung verwenden (wenn der Händler PSC aktzepiert).

Bei der Bezahlung wird man von der Webseite des Händlers zur Webseite von Paysafecard weiter geleitet. Dort gibt man den gekauften Code ein und der Händler erhält die Information, dass die Bezahlung erfolgt ist. Es ist nicht notwendig, dass man einen Gutscheincode genau mit dem geforderten Betrag vorweisen kann. Man kann mehrere Gutscheine für eine Bezahlung verwenden oder nur einen Teilbetrag von Gutschein einlösen. Der Restbetrag bleibt erhalten und kann später verwendet werden.

Eine Paysafecard ist 12 Monate uneingeschränkt gültig. Danach werden für jeden weiteren Monat 2 Euro vom Guthaben abgezogen. Es ist also sinnvoll, kleinere Guthaben bei Bedarf zu kaufen. Das verhindert auch eine technisch mögliche Verkettung mehrerer Einkäufe über den gleichen Gutscheincode.

Nach praktischen Erfahrungen von sind die Verkäufer im Supermarkt, Tankstellen u.ä. nicht immer über die angebotene Möglichkeit des Verkaufes von Paysafecard Gutscheinen informiert. Hartnäckig bleiben und die Verkäuferin auf das Paysafecard Symbol im GUI der Kasse hinweisen hilft.

Durch Verschärfung der Sicherheitsvorkehrungen im April 2012 kommt es häufig zu gesperrten Gutscheinen, wenn die Gutscheine von verschiedenen IP-Adressen genutzt oder abgefragt werden. Nachfragen beim Support von Paysafecard, wie man die Sperrung der Gutscheincodes vermeiden kann, wurden bisher nicht beantwortet. Wenn ein Gutschein gesperrt wurde, muss man sich an den Support von Paysafecard wenden. Restbeträge kann man sich unter Angabe der eigenen Kontonummer erstatten lassen.

Aufgrund des Gesetzes gegen Geldwäsche ist Paysafecard gezwungen, die Anonymität des Zahlungsmittels einzuschränken. Deutsche Nutzer sollen (aber müssen nicht) auf der Website unter *"My PaySafaCard"* einen Account erstellen und können diesen Account mit Gutscheincodes aufladen. Wer mehr als 100,- Euro pro Monat nutzen möchte, muss sich mit Ausweisdokumenten identifizieren. Probleme mit gesperrten Gutscheinen soll es dann nicht geben.

Eine Nutzung von mehreren Gutscheinen mit Restbeträgen für einen Bezahlvorgang ist seit Sept. 2012 NICHT mehr möglich! Restbeträge kann man sich unter Angabe der Kontonummer erstatten lassen. Damit wird die Anonymität des Zahungsmittels leider ausgehebelt. Passende Paysafecards gibt es nicht immer, es gibt nur Gutscheine für 10, 15, 20, 25, 30, 50 oder 100 Euro.

Seit Ende Oktober 2014 sperrt paysafecard Anonymisierungsdienste. Will man bei der Bezahlung anonym bleiben und nutzt einen Anonymisierungsdienst wie Tor, dann erhält man eine Fehlermeldung. Der Gutschein Code wird bei 1-2 Versuchen nicht gesperrt, man kann ihn ohne

Anonymisierungsdienst weiter verwenden.

- **UKash:** funktioniert ähnlich wie Paysafecard, bietet aber nicht ganz so viele Verkaufsstellen in Deutschland. Im Gegensatz zu Paysafecard sind keine Probleme mit gesperrten Gutscheincodes bekannt. Außerdem wird man bei UKash nicht zur Einrichtung eines Accounts gedrängt. Die Nutzung ist damit anonymer, als mit Paysafecard.

  UKash akzeptiert keine Anonymisierungsdienste und VPN-Dienstleister als Partner, hat aber mit (illegalen) Webseiten zu (Sport-) Wetten kein Problem:

  > *Ukash will not under any circumstances knowingly approve Merchants associated directly or indirectly with the following products or services:*
  > .....
  > *l. IP anonymisers or private VPNs or any similar service which has the intention of hiding the true identity of a computer or device.*

- **Pecunix:** wickelt Bezahlungen in Gold ab. Die Geldbeträge werden automatisch in Gold konvertiert. Um mit Pecunix zu bezahlen, ist ein Account zu erstellen, bei dem ebenfalls lediglich die E-Mail Adresse gültig sein muss. Als einziger Bezahldienstleister kann Pecunix den gesamten E-Mail Verkehr zu den Nutzern mit OpenPGP verschlüsseln. Man kann seinen eigenen OpenPGP-Schlüssel im Account hochladen und die Option zur Verschlüsselung aktivieren.

  Um mit Pecunix bezahlen zu können, muss man eGold kaufen. Auf der Webseite von Pecunix findet man einen Liste von Exchangern.

- **cashU:** ist ein Bezahlservice, der hauptsächlich in der arabischen Welt verwendet wird. Registrieren kann man sich *wie man will* und die Konten bleiben unüberprüft bestehen. Die cashU Währung lässt sich auf der Webseite durch UKash Codes aufladen, wenn man sich mit einer Kopie des Ausweises identifiziert. Einen anderen Weg habe ich von Deutschland aus noch nicht gefunden.

5.5 Anonyme Online-Zahlungen vor dem Aus?

Die Bundesregierung bereitete unter dem Deckmantel des Kampfes gegen Geldwäsche ein Gesetz vor, das für anonyme Bezahlungen im Internet das Aus bedeutet hätte. Künftig sollen Verkaufsstellen von Paysafecards und UKash Vouchers die Käufer identifizieren und die Daten für eine mögliche Prüfung 5 Jahre bereithalten. Im Gegensatz zu Bareinzahlungen, die statt bisher ab 15.000 Euro zukünftig ab 1.000 Euro berichtspflichtig werden, sollten für E-Geld keine Mindestgrenzen gelten.[7]

[7] http://heise.de/-1269409

Nach Ansicht von Udo Müller (Paysafecard-Geschäftsführer) wären diese Anforderungen auch für die Vertriebsstruktur das AUS. 95% der Partner wie Tankstellen, Geschäfte usw. würden unter diesen Bedingungen den Verkauf von Paysafecard Gutscheinen und UKash Vouches einstellen.

Unklar ist, wie die bei E-Geld üblichen Kleinbeträge in nennenswertem Umfang für Geldwäsche genutzt werden können. Die Regierung hat dafür keine sinnvolle Erklärung geliefert. Nach den vom BKA vorgelegten Zahlen zum Missbrauch von Prepaidkarten zur Geldwäsche ist der Missbrauch sehr gering. Nur in 94 von 14.000 Verdachtsfällen, die gemeldet wurden, spielten Prepaidkarten eine Rolle. Das sind 0,7% aller Verdachtsfälle. Der Bundesdatenschutzbeauftragte Schaar hat sich gegen den Entwurf ausgesprochen:

> *Ich appelliere an den Gesetzgeber, den überzogenen Ansatz der neuen Vorschläge entsprechend zu korrigieren.*

Die 82. Konferenz der Datenschutzbeauftragten Ende September 2011 verfasste zu diesem Gesetzentwurf eine Stellungnahme:

> *Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht in Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts.*

Am 01. Dez. 2011 hat der Deutsche Bundestag das Gesetz in einer etwas entschärften Version beschlossen. Für den Kauf von Prepaidkarten bis 100 Euro ist keine Identifizierung der Käufer nötig. Für Prepaidguthaben von mehr als 100 Euro sind die Käufer zu identifizieren. Die Daten sind 5 Jahre lang zu speichern. Der Bundesdatenschutzbeauftragte kommentierte die Verabschiedung des Gesetzes u.a. mit folgenden Worten:

> *So begrüßenswert es ist, dass der anonyme Erwerb von E-Geld damit nicht generell abgeschafft wird, so kritisch sehe ich die nach wie vor bestehende Tendenz, individuelles Handeln in immer stärkerem Maße zu registrieren...*
>
> *Die Diskussion über Identifikationspflichten - vor allem bei der Inanspruchnahme des Internets - ist damit aber sicherlich noch nicht beendet.*

Der EU-Rat hat im Dez. 2016 in den *Verhandlungspositionen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung*[8] die Gangart deutlich verschärft und fordert die **Aufhebung der Anonymität von virtuellen Währungen** wie Bitcoin u.ä. Die Umtausch-Plattformen für virtuelle Währungen und Anbieter elektronischer Geldbörsen müssen zukünftig gemäß den Richtlinien für Banken die Identität ihrer Kunden verifizieren. Die Umsetzung in nationale Gesetze soll 2017 in allen EU-Ländern erfolgen.

[8] http://www.consilium.europa.eu/de/press/press-releases/2016/12/20-money-laundering-and-terrorist-financing/

5.6 Bargeld

Man kann im Internet nicht mit Bargeld bezahlen, trotzdem soll es kurz erwähnt werden, weil das anonyme Bezahlen mit Bargeld schrittweise immer weiter eingeschränkt wird. Angesichts der ungebremsten Schuldenentwicklung und unzureichenden Wachstums wird die Politik immer radikalere Maßnahmen ergreifen. Ein Bargeldverbot passt durchaus ins Konzept.

In Italien, Spanien, Frankreich, Griechenland und Zypern wurden Bargeldzahlung über einen Höchstsatz von 1.000-3.000 Euro bereits verboten, in Frankreich wird ab August 2015 die Höchstgrenze für Bezahlung mit Bargeld auf 2.000 Euro abgesenkt (das Gesetz wurde nach dem Charlie-Hebbo-Attentat verabschiedet). In Dänemark wurde ein Gesetz aufgehoben, das Läden im Einzelhandel zwingt Bargeld akzeptieren müssen, außerdem wird die dänische Notenbank ab 2016 keine Geldscheine mehr drucken.

Der Wirtschaftsweise Bofinger und der US-Ökonom Rogoff haben im Mai 2015 nachdrücklich die Abschaffung des Bargelds gefordert. Sie appellierten an Bundeskanzlerin Merkel, dass Sie sich auf dem G7-Gipfel in Elmau für eine weltweite Abschaffung des Bargeld einsetzen soll. Dafür wurden folgende Gründe genannt: [9], die ich nur kurz kommentieren will:

Stärkung der Nationalbanken: Wollen wir wirklich irgendwelche Banken stärken? Wir sollten lieber über die Einführung von Vollgeld diskutieren (wie in Island oder in der Schweiz), um die Macht der Banken zu brechen und Banken auf ihren eigentliche Funktion zurück zu führen.

Austrocknung des Schwarzmarktes: Schwarzmarkt == BÖSE (Drogen, Kipo werden genannt - klar)

Der Schwarzmarkt ist aber auch ein Regulativ zwischen der Gesetzgebung und den Bürgern. Wenn eine Regierung die Wünsche der Bürger konsequent missachtet, dann haben Bürger die Möglichkeit, auf den Schwarzmarnkt auszuweichen (natürlich unter Androhung von Strafen). Je drakonischer und unbeliebter die Finanzgesetze werden, desto stärker wird der Schwarzmarkt wachsen.

Die Austrocknung des Schwarzmarktes wird also auch die Macht der Regierenden und Banken gegenüber der Bevölkerung stärken. Wollen wir diese Entwicklung?

Negativzinsen durchsetzen: *Die Zentralbanken könnten auf diese Weise leichter Negativzinsen durchsetzen. Papiergeld ist das entscheidende Hindernis, die Zentralbank-Zinsen weiter zu senken. Seine Beseitigung wäre eine sehr einfache und elegante Lösung für dieses Problem.* (US-Ökonom Rogoff)

Das würde bedeuten, dass sich die Sparer gegen diese Enteignung nicht mehr wehren könnten, indem sie das Geld einfach abheben. Einen soge-

[9] http://www.manager-magazin.de/finanzen/artikel/bofinger-und-rogoff-fordern-abschaffung-des-bargelds-a-1034135.html

nannter Bankenrun (wenn Kunden massenweise ihr Geld abheben) will keine Bank riskieren.

Kommentare zu den Vorschlägen von Bofinger/Rogoff

> *Um diese beiden Argumente ernsthaft als Vorteile durchgehen zu lassen, muss man ein Technokrat sein, der einen lückenlos organisierten Ameisenhaufen für die beste aller Gesellschaften hält. Wer Freiheit, Bürgerrechte und eine lebendige Demokratie bewahren will, den muss es schütteln, wenn jemand, der als Weiser gilt, solche Ansichten verbreitet.*[10]

Noch etwas deutlicher:

> *Es geht dem ehemaligen Chefökonomen des Internationalen Währungsfonds (IWF) und dem IWF längst neben einer umfassenden Kontrolle der Bevölkerung auch darum, die Grundlage für die finanzielle Repression zu schaffen, um die ausufernde Verschuldung über die Enteignung der Sparer zu lösen.*[11]

Forderungen deutscher Politiker

- Der NRW-Finanzminister Walter-Borjans (SPD) beteiligt sich an der Kampagne gegen Bargeld und forderte im Juli 2015 eine Obergrenze bei Barzahlung. Bezahlungen mit Bargeld sollten in Deutschland nur bis 2.000 - 3.000 Euro erlaubt sein. Ein höherer Betrag würde ihn skeptisch machen. (Warum eigentlich?)

- Der NRW Landeschef des Bundes Deutscher Kriminalbeamter (BDK), Sebastian Fiedler, unterstützt. Fiedler behauptet, wenn man 70.000 Euro für ein Auto oder 200.000 Euro für eine Immobilie bar bezahlt, dann handelt es sich um Geld aus Steuerhinterziehung oder Straftaten. (Kann man ein Auto anonym zulassen oder eine Immobilie anonym ins Grundbuch eintragen lassen und die Verwendung illegaler Einnahmen damit geheim halten? Wer findet den Denkfehler?)

- Im Januar 2016 wurde ein Plan der Bundesregierung bekannt, europaweit die Obergrenze für Barzahlungen auf max. 5.000 Euro festzulegen, um die Finanzierung von Terrorismus zu unterbinden. Da diese Forderung in Deutschland nur schwer durchsetzbar ist und auch von Finanz- und Datenschutzexperten abgelehnt wird, versucht die Bundesregierung wieder einmal den Weg über die EU.

- Außerdem fordert W. Schäuble zentrale Bankkontenregister in allen Mitgliedsstaaten der EU und die bessere Kontrolle von anonymen Prepaid-Zahlungsmittel und Kryptowährungen wie Bitcoin und Ripple zur *Terrorbekämpfung*.

[10] http://bitcoinblog.de/2015/05/18/bargeld-ist-macht
[11] http://www.heise.de/tp/artikel/45/45089/1.html

Kommentare zu den Forderungen deutscher Politiker

- Wer etwas gegen die Finanzierung von Terrorismus tun will, der sollte die Beziehungen zu den Staaten wie Saudi Arabien, Katar oder USA überdenken, die als weltweit als die größten Finanzgeber von Terroristen bekannt sind. Man könnte auch Druck auf die Türkei ausüben, um die Verkaufswege von Erdöl aus den von der ISIS besetzten Gebieten zu unterbinden und damit eine wesentliche Geldquelle des ISIS treffen.

- Sicher kommt es vor, dass gelegentlich ein Köfferchen mit Bargeld den Besitzer wechselt. Der Waffenschieber Schreiber hat beispielsweise im Namen von Thyssen-Krupp der CDU eine Spende von 1,3 Mio. D-Mark in einem Köfferchen übergeben, dass die CDU nicht ordnungsgemäß versteuerte. Er hat W. Schäuble 100.000 D-Mark in Bar geschenkt, die ebenfalls nicht korrekt verbucht und versteuert wurden. Deshalb trat unser jetziger Finazminister vom CDU Parteivorsitz zurück und musste Merkel den Vortritt lassen. Derartige Praktiken wird man durch eine 5.000 Grenze für Barzahlungen aber nicht wirklich verhindern können.

- Die Steuerfahndung hat in Deutschland aber ganz andere Probleme. Der Fall Zumwinkel ist schönes Beispiel. Der Steuerfahnder wurde von seinen Vorgesetzten ausdrücklich angewiesen, den Fall Zumwinkel nicht weiter zu verfolgen. Er tat es trotzdem und wurde dafür mit einem psychologischen Gutachten vom Dienst suspendiert. Die Staatsanwältin, die den Fall mit über 1 Mio Euro Steuerbetrug vor Gericht brachte, wurde strafversetzt. Die Anklage wurde verzögert, bis ein Teil der Steuerschuld verjährt war und die Summe des Betruges unter 1 Mio Euro lag. Mehr kann man in dem Buch Inside Steuerfahndung (ISBN: 978-3-86883-105-4) von Frank Wehrheim und Michael Gösele nachlesen. Die Probleme liegen jedenfalls nicht in der Verfügbarkeit von Bargeld.

Weitere Entwicklung

In Deutschland werden lt. einer Studie der Bundesbank[12] noch 53% der Umsätze im Einzelhandel in Bargeld abgewickelt. Außerdem steht eine Mehrheit der Deutschen Experimenten mit Zahlungssytemen eher skeptisch gegenüber. Nach Einschätzung der Bundesbank ist derzeit eine Abschaffung von Bargeld nicht möglich. Diese Zahlen zeigen auch, wie man sich gegen diese Bestrebungen wehren kann:

Verwendet Bargeld, wo es möglich ist.

Der unabhängige Finanzanalyst Martin Armstrong ist der Meinung, dass der Euro mittelfristig mit 90% Wahrscheinlichkeit **nicht** bestehen bleiben wird. Eine Währungsreform wird der Staat auch zur Teilenteignung der Sparguthaben und zur Senkung seiner eigenen Schulden nutzen wollen. Nach Meinung von Armstrong muss das Finanzsystem in regelmäßigen Abständen vollständig crashen, weil die Staaten als Haupschuldner nie vorhaben, ihren Schulden vollständig zurück zu zahlen, sondern in einem gigantischen Ponzischema immer neue Schulden aufnehmen, um Zinsen abzuzahlen. Die

[12] http://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Bericht_Studie/zahlungsverhalten_in_deutschland_201

Alternative zum Finanzcrash wäre ein Krieg.

Das österreichisch-deutschen Unternehmen EDAQS hat mit Hilfe von RFIDs Geldscheine entwickelt, die ferngesteuert entwertet werden können[13]. Das ist eine weitere, beunruhigende Entwicklung. Neben der ferngesteuerten Entwertung von Geldscheinen nach einem Bankraub soll damit auch die Finanzierung von *Terrorgruppen* verhindert werden können (ok - das scheint sich zum Universalargument zu entwickeln). Außerdem wäre es damit möglich, Sparguthaben unter der Matraze (außerhalb des Zugriffs der Banken) bei Bedarf und natürlich nur auf Basis gesetzlicher Grundlagen zu entwerten.

5.7 Bitcoin

Bitcoin ist eine digitale Peer-2-Peer Währung ohne zentrale Verwaltung. Sie ist unabhängig von der Geldpolitik einer Zentralbank und entwickelt sich marktgetrieben durch die Aktivitäten der Teilnehmer, die Bitcoin als Zahlungsmittel akzeptieren oder verwenden.

Die Wurzeln der ökonomischen Theorie dieser virtuellen Währung liegen in der *Austrian school of economics*, die von den Ökonomen Eugen v. Böhm-Bawerk, Ludwig Mises und Friedrich A. Hayek entwickelt wurde. Die Ökonomen kritisieren das gegenwärtige System des Fiatgeldes der Zentralbanken. Sie sehen in den massiven, politisch motivierten Interventionen der Zentralbanken in den Geldumlauf eine wesentliche Ursache für den Krisenzyklus. Als Ausweg empfehlen sie eine Internationalisierung der Währungen und die Rückkehr zum Goldstandard.

Gegenwärtig ist Bitcoin der populärste Versuch zur Umsetzung einer Währung in Anlehnung an die Konzepte der *Austrian school of economics*. Die Software löst mit kryptografischen Methoden vor allem zwei Probleme:

1. Das Kopieren und mehrfache Verwendung der Bits und Bytes, die ein Coin repräsentieren, ist nicht möglich.
2. Die Gesamtmenge der verfügbaren Coins ist limitiert. Neue Bitcoins werden nach einem festen Schema generiert und die Gesamtzahl ist limitiert.

Darauf aufbauend kann Bitcoin als Bezahlmethode verwendet werden. Bitcoins lassen sich in reale Währungen hin- und zurücktauschen. Der Kurswert der Bitcoins beim Tausch gegen reale Währungen (z.B. Euro) ergibt sich dabei ausschließlich aus dem Markt. Die Bezahlungen können relativ schnell am PC abgewickelt werden. Es dauert in der Regel nur 30-60min, bis das Bitcoin Netzwerk eine Transaktion hinreichend bestätigt hat.

Viele Dienste im Netz akzeptieren Bitcoins als Bezahlung. Eine Übersicht findet man im Bitcoin Wiki [14]. Man kann Musik, E-Books, Web- und Mailhosting oder Anonymisierungsdienste / VPN-Anbieter mit Bitcoins bezahlen.

[13] http://www.t-online.de/wirtschaft/boerse/devisen/id_74134666/geldscheine-koennen-bald-per-funk-entwertet-werden.html
[14] https://en.bitcoin.it/wiki/Trade

Der Kurs wird dabei von jedem Anbieter selbst festgelegt. Dabei kann es vorkommen, dass Anbieter vom mittleren Tauschkurs abweichen. Die schnelle, unkomplizierte Bezahlung bei Webdiensten, die die Privatsphäre ihrer Kunden respektieren, ist für mich die Hauptanwendung von Bitcoin. Es ist praktisch, wenn man immer ein paar Bitcoins im Wallet hat und unkompliziert bezahlen kann.

Um mit Bitcoins zu bezahlen, braucht man selbst ein paar Bitcoins. Diese kann man auf verschiedenen Markplätzen gegen reale Währung kaufen oder man bietet selbst Dienstleistungen gegen Bitcoins als Bezahlung an. Bei den Bitcoin Meetups in fast allen größeren Städten trifft man mit Sicherheit Verkäufer von Bitcoins, die anonym Coins gegen Cash verkaufen.

5.7.1 Exchanger / Marktplätze

Man kann Bitcoin komplett ohne Installation einer Software nutzen. Es gibt Webdienste (die sogenannten Exchanger oder Markplätze), die den Handel mit Bitcoins zwischen den Personen einleiten und eine Bitcoin Brieftasche (eWallet) für Nutzer bereitstellen. Das vereinfacht die Nutzung von Bitcoin als Zahlungsmittel, da eine Installation von Software nicht zwingend nötig ist. Die erworbenen Bitcoins können aber auch auf den eigenen PC transferiert und mit einem Bitcoin Client verwaltet werden (z.B. mit Electrum).

Die Exchanger verifizieren die Identität der Nutzer. Eine anonyme Nutzung ist nicht möglich. Hinweise zum anonymen Kauf von Bitcoins gibt es weiter unten im Abschnitt *Anonymität von Bitcoin*.

Warnung: viele Markplätze haben sich als unsicher erweisen. Das prominenteste Beispiel ist die Insolvenz von *MtGox* nachdem Bitcoins im Wert von 368,4 Millionen Euro verloren gingen. Viele Kunden, die mit Bitcoin als Spekulationsobjekt das große Geld gewinnen wollten, haben ihr Geld dort verloren. Weitere Beispiele sind die Bitcoin Börsen *Flexcoin* (die nach virtuellem Bankraub geschlossen wurde) oder *Poloniex*. Man sollte also gut überlegen, ob man seine Bitcoin Brieftasche einem Fremden anvertraut oder ob man sie lieber selbst verwaltet.

ür den Einstieg war Bitcoin.de als Marktplatz früher mal gut geeignet. Im Gegensatz zu anderen Marktplätzen ist der Handel bei Bitcoin.de durch Kooperation mit der Fidor-Bank abgesichert. Allerding muss man jetzt das Bankkonto durch Überweisung von 1 Cent via SOFORT Überweisung verifizieren, bevor man dort Bitcoins kaufen kann (siehe FAQ). Außnahmen gibt es nur in besonderen Ausnahmefällen. Das gefällt mir überhaupt nicht, ich werde SOFORT Überweisung nicht nutzen, da der Dienst ein Sicherheitsrisiko ist.

Ich kenne im Moment keinen Online Marktplatz für Bitcoins, den ich empfehlen kann.

5.7.2 Bitcoin Software

Wenn man einem externen Webserver nicht vertraut, kann man seine Bitcoins lokal auf dem eigenen Rechner oder Smartphone verwalten. Dafür muss ein Bitcoin Client wie Bitcoin-Qt oder Electrum installiert werden.

Bitcoin-Qt ist der Standard Client des Bitcoin Projektes und steht zum Download unter http://bitcoin.org/en/download bereit. Er ist einfach bedienbar, bietet eine Übersicht über alle Transaktionen und kann beliebig viele Adressen verwalten.

Ein Nachteil für Gelegenheitsnutzer ist der ständige Download der gesamten Blockchain. Die Downloadseite weist darauf hin, dass die erste Initialisierung bis zu einem Tag dauern kann. Wenn man nach 3-4 Wochen Pause wieder einmal mit Bitcoins bezahlen möchte, dann benötigt Bitcoin-Qt ein bis zwei Stunden für die Aktualisierung der Blockchain, um wieder arbeitsbereit zu werden.

Electrum ist eine leichtgewichtige Alternative für Gelegenheitsnutzer. Es überlässt die Hauptarbeit speziellen Servern im Netz und benötigt die komplette Blockchain nicht. Trotzdem ist sichergestellt, dass die privaten Schlüssel ausschließlich in der Verfügung des Anwenders liegen. Die Installation für unterschiedliche Betriebssysteme ist auf der Website https://electrum.org unter *Download* beschrieben.

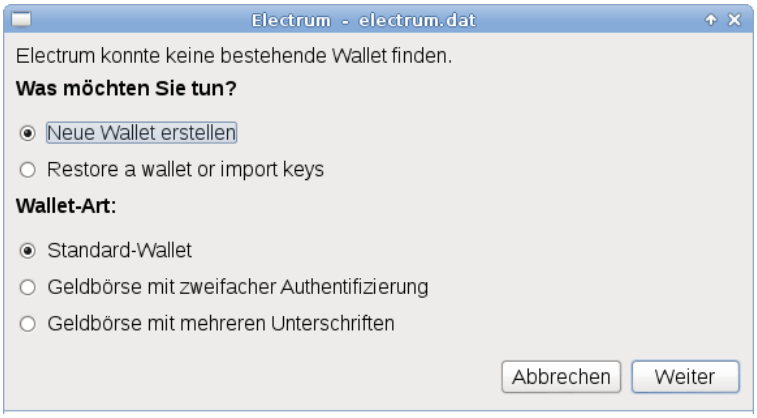


Abbildung 5.1: Neues eWallet in Electrum erstellen

Beim ersten Start fragt Electrum, ob ein neuer Account erstellt werden soll oder ob ein Wallet mit dem Backup eines vorhandenen Seed wieder hergestellt werden soll (Bild. 5.1). Ein Standard Wallet kann man mit einem Passwort schützen. Wenn man ein Wallet mit zweifacher Authentifizierung wählt, dann muss der Service TrustedCoin[15] alle Transaktionen unterschreiben. Gegenüber TrustedCoin authentifiziert man sich mit einem One-Time-Passwort.

[15] https://api.trustedcoin.com/

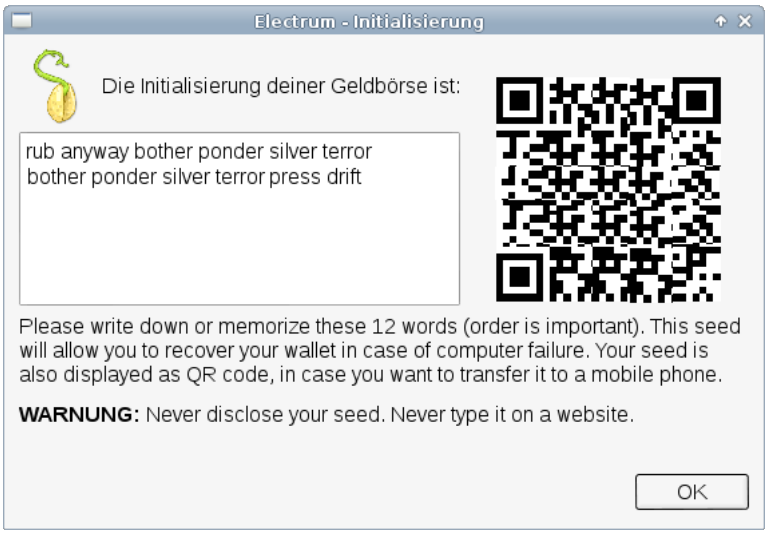


Abbildung 5.2: Seed exportieren

Im nächsten Schritt wird bei der Erstellung eines neues eWallet der Seed angezeigt. Mit dem *Seed* kann das eWallet jederzeit auf einem anderen Rechner aus dem *ewigen Logfile* rekonstruiert werden. Ein vollständiges Backup der Konfiguration ist nicht nötig. Man benötigt nur den Seed, der wie eine lange Passphrase aus 25 Worten besteht. Der Seed ist unbedingt zu speichern (z.B. in einer verschlüsselten Passwortdatenbank wie KeepassX). Mit dem QR-Code könnte man den Seed schnell auf ein Smartphone übertragen, wenn man das gleiche Wallet auch unterwegs (in der realen Welt) nutzen möchte.

Die Oberfläche von Electrum ist einfach gehalten. Für die Übersicht der Transaktionen, zum Senden und Empfangen sowie eine einfache Adressliste gibt es Reiter im Hauptfenster (Bild 5.3).

Die Netzwerkeinstellungen öffnet man mit einem Klick auf das rechte Icon in der Statusleiste im Hauptfenster, dass üblicherweise ein grüner Punkt ist. Hier kann man festlegen, welchen Server man für die rechenintensiven Aufgaben nutzen möchte. Der Server kann aus der Liste frei gewählt werden, da keine Accountdaten auf dem Server gespeichert werden. Die Server werden durch Spenden finanziert und die Betreiber sind für eine kleine Spende in Bitcoins dankbar. Die Spendenadresse für den aktuell genutzten Server findet man auf dem Reiter *Console*.

Außerdem kann man in den Netzwerkeinstellungen den Proxy konfigurieren. Da Electrum nur geringen Datenverkehr verursacht, ist eine sinnvolle Kombination mit den Anonymisierungsdiensten Tor Onion Router möglich. Folgenden Proxy Einstellungen sind für Tor zu wählen:

- TorBrowserBundle: SOCKS5, localhost, 9150
- Tor (stand alone): SOCKS5, localhost, 9050

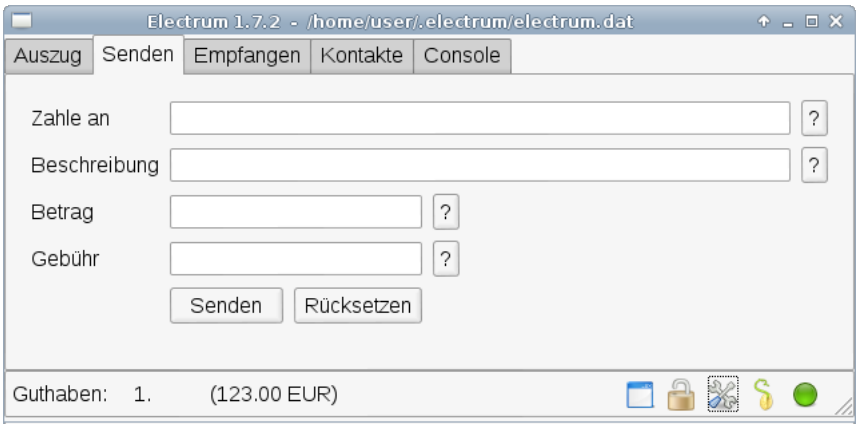


Abbildung 5.3: Hauptfenster von Electrum

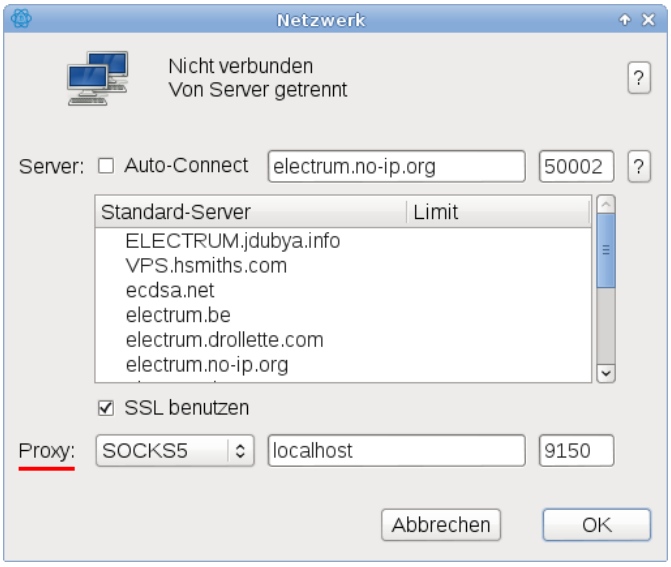


Abbildung 5.4: Proxy Konfiguration in Electrum

5.7.3 Anonymität von Bitcoin

Über die Anonymität von Bitcoin gibt es viele Missverständnisse.

Alle Bitcoin Transaktionen werden in der öffentlich zugäglichen Blockchain protokolliert (ein *ewiges Logfiles*). Das ist kein Designfehler sondern notwendig, um double spending zu verhindern.

- Forscher der TU Darmstadt haben auf dem 28C3 eine Analyse des *ewigen*

Logfile von Bitcoin vorgestellt [16]. Eine weitere Analyse wurde von D. Ron und A. Shamir publiziert [17]. Beide Analysen konnten scheinbar unabhängige Bitcoin Adressen zusammen führen und die IP-Adressen von Nutzern ermitteln. Dazu zählen beispielsweise Spender, die an Wikileaks via Bitcoin gespendet haben. Außerdem wurden Zahlen zur Bitcoin Nutzung von Wikileaks als Beispiel veröffentlicht. Bis März 2012 nutzte Wikileaks 83 Bitcoin Adressen und erhielt 2605.25 BTC von Unterstützern.

- In dem wiss. Paper *Deanonymisation of clients in Bitcoin P2P network* [18] wird ein Angriff auf Netzwerkebene vorgestellt, der orthogonal zu den Angriffen durch Auswertung der Blockchain ist und zur Deanonymiserung von Bitcoin Usern im Tor Netzwerk verwendet werden kann.

Die Forscher kommen zu dem Schluss, dass die Anonymität von Bitcoin geringer ist, als eine einfache Banküberweisung.

Die Europäische Zentralbank (EZB) sieht laut einem Bericht von Okt. 2012 in Bitcoin eine Gefahr, da es außerhalb der Kontrolle der Zentralbanken läuft und empfahl schon damals eine intensivere Beobachtung. Der EU-Rat hat im Dez. 2016 in den Verhandlungspositionen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung die Gangart deutlich verschärft und fordert die Aufhebung der Anonymität von virtuellen Währungen wie Bitcoin u.ä. Die Umtausch-Plattformen für virtuelle Währungen und Anbieter elektronischer Geldbörsen müssen zukünftig gemäß den Richtlinien für Banken die Identität ihrer Kunden verifizieren. Die Umsetzung in nationale Gesetze soll 2017 in allen EU-Ländern erfolgen.

Die Firma Chainanalysis bietet Banken, Strafverfolgung, Geheimdiensten u.ä für $500 pro Monat eine API mit Real-Time Informationen zur Beobachtung aktuellen Transaktionen in der Blockchain. Ziel der Firma ist es, compliance mit geltenden Gesetzen zur Überwachung von Finanzströmen herzustellen. Über die API ist es möglich, scheinbar unabhängigen Bitcoin Adressen auf einen Nutzer zurück zu führen, Nutzer zu identifizieren oder *known bad actors* gezielt zu überwachen. Die geleakte Roadmap von Chainanalysis zeigt, wie es weitergehen soll. Automatisiertes Profiling der Nutzer steht auf der Liste und eine Gruppierung der Payment Prozessoren in Gruppen wie *dark markets, gambling sites*....

Das sich Geheimdienste für Bitcoin Transaktionen interessieren, kann man auch dem Trojaner RCS der italienischen Firma Hacking Team sehen. Der Trojaner, der u.a. gegen politische Aktivisten und Dissidenden eingesetzt wurde, enthält ein *Money Module*, das alle Transaktionen von Bitcoin, Litecoin, Feathercoin und Namecoin analysieren kann.[19]

[16] http://events.ccc.de/congress/2011/Fahrplan/events/4746.en.html
[17] http://eprint.iacr.org/2012/584
[18] http://arxiv.org/abs/1405.7418
[19] https://bitcoinmagazine.com/21246/italian-spyware-tracks-bitcoin-transactions-private-keys/

Bitcoin ist im Zeitalter der Überwachung angekommen. Man kann davon ausgehen, das Bitcoin zukünftig in gleichem Maße überwacht wird wie Kontobewegungen oder Kreditkarten.

5.7.4 Bitcoin anonym nutzen

Da das gesamte System von Bitcoin auf Informationsaustausch im Internet basiert, ist es mit Anonymisierungsdiensten möglich, Bitcoin auch vollständig anonym zu nutzen. Dabei sind folgende Punkte zu beachten:

Bitcoin-Brieftasche anonym verwalten: Man kann einen Webservice verwenden und mit dem *TorBrowserBundle* das eWallet anonym auf den Servern verwalten. (Hinweis: Dabei legt man seine Brieftasche in die Hand eines Fremden, ist also eher für kleinere Beträge geeignet.)

- Blockchain.info[20] bietet die Verwaltung eines anonymen eWallet auf dem Webserver und erfordert keine persönlichen Angaben bei der Registrierung.
- StrongCoin.com[21] erfordert die Angabe einer E-Mail Adresse bei der Registrierung. Wegwerfadressen werden akzeptiert. Das Webinterface ist für Smartphones geeignet.
- OnionBC ist ein anonymer eWallet Service, der nur als Tor Hidden Service unter 6fgd4togcynxyclb.onion erreichbar ist. (Ich bin immer etwas skeptisch bei Tor Hidden Services. Wenn man nicht weiss, wer den Dienst betreibt, kann es sich oft um Scam handeln. TORwallet hat sich z.B. als Scam herausgestellt.)

Wenn man einem Webdienst nicht vertrauen möchte, kann man den Bitcoin Client *Electrum* installieren und den Datenverkehr mit Tor Oinion Router anonymisieren. Electrum überlässt die Hauptarbeit speziellen Servern und muss deshalb nicht das *ewige Logfile* ständig aktualisieren. Das reduziert den Datenverkehr und ermöglicht eine sinnvolle Kombination mit Tor. Die privaten Schlüssel bleiben aber immer auf dem eigenen Rechner.

Bitcoins anonym kaufen: Man kann beim Kauf von Bitcoins die Angabe eines Bankkontos oder anderer identifizierender Informationen vermeiden.

- Auf der Webseite LocalBitcoins.com[22] findet man Anbieter in der Umgebung, die Bitcoins gegen Bargeld verkaufen.
- Im IRC Channel #bitcoin-otc im Freenode Netz kann man beliebige Formen der Geldübergabe mit dem Verkäufer vereinbaren.
- In Berlin trifft sich die Bitcoin Community an jedem ersten Donnerstag im Monat im *room 77* (Graefestr. 77, 10967 Berlin-Kreuzberg). Dort findet immer jemanden, der Bitcoins gegen Bargeld verkauft.

[20] https://www.blockchain.info/wallet
[21] https://www.strongcoin.com
[22] https://localbitcoins.com/

Bitcoins als Zahlungsmittel verwenden: Beim Einkauf virtueller Güter (z.B. E-Mail Accounts oder eBooks, die per E-Mail zugestellt werden) gibt es keine weiteren Probleme.

Muss man beim Kauf realer Güter eine Lieferadresse angeben, dann sollte man ein anderes Bitcoin eWallet verwenden als für die anonyme Bezahlung virtueller Güter. Anderenfalls könnten auch die anonymen Zahlungen deanonymisiert werden.

Mixing-Services? Im Bitcoin-Wiki werden Mixing-Services wie Blockchain Mixing Service[23] oder Cleanbit.org[24] empfohlen, um die Spuren einer Transaktion zu verwischen. Die Analyse von D. Ron und A. Shamir lässt vermuten, dass diese Mixing-Services mit entsprechendem Aufwand analysiert werden könnten und zukünftig einen potenten Angreifer nicht von einer Verfolgung der Transaktionen abhalten können.

[23] https://blockchain.info/wallet/send-anonymously
[24] http://www.cleanbit.org/

Kapitel 6

E-Mail Kommunikation

E-Mail ist eines der meistgenutzten Kommunikationsmittel. Die folgenden Seiten sollen zum Nachdenken über die die Auswahl des E-Mail Providers anregen und Hinweise für die Konfiguration von Mozilla Thunderbird geben.

Fast alle E-Mail Provider bieten die Möglichkeit, die E-Mail Kommunikation im Webinterface mit einem Browser zu verwalten. Aus mehreren Gründen empfehlen wir aber, die Nutzung eines E-Mail Clients wie z.B. Mozilla Thunderbird zu bevorzugen:

- Der Browser ist eine Sandbox zum Anzeigen von Webseiten. Aufgrund des Funktionsumfangs moderner Browser und der bösartigen Feindlichkeit des Internet muss man von viel mehr Angriffsmöglichkeiten ausgehen, als bei einem Programm, dass speziell für die Bearbeitung von E-Mails optimiert wurde.

- Sichere Ende-zu-Ende Verschlüsselung ist im Browser nicht möglich, auch wenn immer mehr E-Mail Provider Lösungen dafür anpreisen. Alle diese Lösungen haben gegenüber der lokalen Verschlüsselung im E-Mail Client verschiedene Nachteile bei der Sicherheit.

- Einige E-Mail Provider wie WEB.de und GMX.de blockieren nicht alle Tracking Elemente in E-Mails im Webinterface (weil sie selbst Möglichkeiten zum Tracking ihrer Newsletter nutzen). Mit einem E-Mail Client kann man dafür sorgen, dass man seine E-Mails unbeobachtet liest.

6.1 E-Mail Provider

Als erstes braucht man eine oder mehrere E-Mail Adressen. Es ist empfehlenswert, für unterschiedliche Anwendungen auch verschiedene E-Mail Adressen zu verwenden. Es erschwert die Profilbildung anhand der E-Mail Adresse und verringert die Spam-Belästigung. Wenn Amazon, Ebay oder andere kommerzielle Anbieter zu aufdringlich werden, wird die mit Spam überschwemmte E-Mail Adresse einfach gelöscht ohne die private Kommunikation zu stören.

Neben einer sehr privaten E-Mail Adresse für Freunde könnte man weitere E-Mail Adressen für Einkäufe im Internet nutzen oder für politische Aktivitäten. Um nicht ständig viele E-Mail Accounts abfragen zu müssen, kann man die für Einkäufe im Internet genutzten E-Mail Accounts auch an die private Hauptadresse weiterleiten lassen. Alle Mail-Provider bieten diese Option. Bei den großen deutschen Mail Providern GMX.de und WEB.de gibt es bis zu 100 Fun-Domains extra für diesen Zweck. Bereits mit der kostenlosen Version kann man bis zu 3 Fun-Adressen nutzen.

Wenn eine E-Mail Adresse nur für die Anmeldung in einem Forum oder das Veröffentlichen eines Kommentars in Blogs benötigt wird, kann man *temporäre Mailadressen* nutzen (siehe weiter unten).

Eine kleine Liste von empfehlenswerten E-Mail Providern:

- **Mailbox.org** [1] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, PGP verschlüsselte Inbox, verschlüsselter Mailversand und -empfang nur über SSL/TLS aktivierbar, DANE, IP-Adressen der Nutzer und User-Agent werden aus dem Mail Header entfernt, anonyme Accounts möglich, Bezahlung per Brief oder Bitcoin, OTP-Login mit HW-Token und FreeOTP für Webinterface, Tor Hidden Service für POP3, IMAP, SMTP und XMPP)

- **Posteo.de** [2] (deutscher Mailprovider, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, S/MIME oder PGP verschlüsselte Inbox, verschlüsselter Mailversand aktivierbar aber nicht für Empfang, DANE, IP-Adressen der Nutzer werden aus dem E-Mail Header entfernt aber User-Agent Kennung nicht, anonyme Accounts möglich, anonyme Bezahlung per Brief, OTP-Login mit FreeOTP für Webinterface)

- **Mailfence.com** [3] (belgischer Provider, kostenlose Accounts möglich, Premium ab 2,50 Euro pro Monat allerdings mit mehr Speicherplatz als die 1,- Euro Accounts der Mitbewerber, POP3, IMAP und SMTP nur für bezahlte Accounts, OpenPGP im Webinterface möglich mit eigener Implementierung, OTP-Login mit FreeOTP für Webinterface, anonyme Bezahlung via Bitcoin oder ohne Anonymität via Kreditkarte)

- **KolabNow** [4] (Groupware Hosting in der Schweiz mit Adressbuch, Kalender und E-Mail, Mailaccounts für 4.41 CHF pro Monat, Groupware für 10 CHF pro Monat, DANE, IP-Adressen der Nutzer und User-Agent Info werden aus dem E-Mail Header entfernt)

- **neomailbox.com** [5] (anonymes E-Mail Hosting in der Schweiz, Accounts ab $3,33 pro Monat, anonyme Bezahlung mit Pecunix, IP-Adressen der Nutzer werden aus E-Mails entfernt)

[1] https://mailbox.org
[2] https://posteo.de
[3] https://mailfence.com
[4] https://kolabnow.com
[5] http://www.neomailbox.com/services/secure-email

- **aikQ.de** [6] (Mailprovider in GB registriert, Server stehen in Deutschland, Accounts ab 1,- Euro pro Monat, anonyme Accounts möglich mit Bezahlung per Brief, keine 2-Faktor-Auth)
- **runbox.com** [7] (privacy-engagierter norwegischer E-Mail Provider, Server stehen ebenfalls in Norwegen, Accounts ab 1,66 Dollar pro Monat)

Hinweis: es kostet Geld, einen zuverlässigen Mailservice bereitzustellen. Es ist durchaus sinnvoll, die *alles kostenlos Mentalität* für einen vertrauenswürdigen Mailprovider fallen zu lassen.

Sicherheit der SSL/TLS-Verschlüsselung

Die Webinterfaces kann man mit dem *SSL-Test von Qualys SSL Labs*[8] überprüfen. Die Mailserver (SMTP, POP, IMAP) können mit dem Mailserver Test von ssl-tools.net[9] geprüft werden oder mit CheckTLS.com[10]. Dr

- Mailbox.org: sichere Verschlüsselung, DANE
- Posteo.de: sichere Verschlüsselung, DANE
- KolabNow.com: sichere Verschlüsselung, DANE
- Mailfence.com: sichere Verschlüsselung
- aikQ.de: sichere Verschlüsselung
- Runbox.com: sichere Verschlüsselung

Nicht empfohlene E-Mail Provider

Einige Gründe, warum verschiedene E-Mail Provider mit gutem Ruf nicht in die Liste der Empfehlungen aufgenommen wurden:

- Web.de und GMX.de sammeln bei der Registrierung zuviele Daten: Anrede, Vor- und Nachname, Land, PLZ und Ort, Straße und Hausnummer, optional ist nur die Mobilfunknummer für Passwortwiederherstellung.

  Mit der Registrierung erklärt man sich damit einverstanden, dass die Daten für Marketing-Zwecke verwendet werden. Die Daten werden an den Mutterkonzern übermittelt und mit anderen verbundenen Unternehmen geteilt. Außerdem werden die Daten für postalische Werbung genutzt, sie werden für Markt- und Meinungsforschung genutzt und Non-Profit Organisationen für Werbung zur Verfügung gestellt. (Falls man sich schon öfters mal gefragt hat, woher Meinungsforschungsinstitute die eigene Telefonnummer haben....)

[6] https://www.aikq.de
[7] https://secure.runbox.com
[8] https://www.ssllabs.com/ssltest
[9] https://de.ssl-tools.net/mailservers
[10] https://www.checktls.com/

Der EmailPrivacyTest[11] zeit, dass Web.de und GMX.de bei der Nutzung des Web-GUI nicht gegen Tracking Elemente in E-Mails schützen und ermöglichen es damit vielen Diensten, die Nutzer beim Lesen der E-Mails zu beobachten. Web.de setzt selbst HTML-Wanzen in den eigenen Newslettern ein (3 Tracking Wanzen in jedem Newsletter) und verfolgt damit die Lesegewohnheiten der Nutzer.

- Hushmail speichert zuviel Daten. Neben den üblichen Daten beim Besuch der Webseite werden die E-Mails gescannt und folgende Daten unbegrenzt lange gespeichert:

  1. alle Sender- und Empfänger E-Mail Adressen (VDS-artig)
  2. alle Dateinamen der empfangenen und gesendeten Attachements
  3. Betreffzeilen aller E-Mails (nicht verschlüsselbar)
  4. URLs aus dem Text unverschlüsselter E-Mails
  5. ... and any other information that we deem necessary

  Diese Daten werden bei der Kündigung eines Account NICHT gelöscht.

  Bei der Bezahlung für einen Premium-Account werden die IP-Adresse des Kunden sowie Land, Stadt und PLZ an Dritte weitergeben. Außerdem bindet Hushmail.com Dienste von Drittseiten ein. Die ID des Hushmail Account wird beim Besuch der Webseite nach dem Login an diese Drittseiten übermittelt. Für die Privacy-Policy dieser Drittseiten übernimmt Hushmail.com keine Verantwortung.

- In der EU-Studie *Fighting cyber crime and protecting privacy in the cloud*[12] warnen die Autoren in Kapitel 5.4 (S. 48) vor Risiken bei der Speicherung von Daten in den USA. Aufgrund des *US PATRIOT Act* (insbesondere S. 215ff) und der *4. Ergänzung des FISA Amendments Act* ist es für US-Behörden ohne juristische Kontrolle möglich, die Kommunikation von Nicht-US-Bürgern zu beschnüffeln. Dabei ist es unerheblich, ob der Cloud- bzw. E-Mail Provider eine US-Firma ist oder nicht. Es reicht nach Ansicht der Amerikaner, wenn die Server in den USA stehen.

  Außerdem hat US-Präsident Trump als eine seiner ersten Handlungen die Behörden in den USA per Dekret aufgefordert, den Datenschutz für Ausländer vollständig aufzuheben. Es ist unklar, welche Auswirkungen das Dekret und die damit angedeutete Richtung im Datenschutz zukünftig für EU-Bürger haben wird.[13].

  Aus diesem Grund ist ein Server-Standort *USA* für deutsche Nutzer eher ungeeignet. Das betrifft u.a. die E-Mail Provider SecureNym, S-Mail, Fastmail.fm, Rise-up.net...

- Weitere Beispiele werden auf der Webseite des Handbuches genannt.[14]

[11] https://www.emailprivacytester.com
[12] http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050
[13] https://netzpolitik.org/2017/datenschuetzer-raetseln-schafft-trump-datenschutz-abkommen-zwischen-usa-und-eu-ab/
[14] https://www.privacy-handbuch.de/handbuch_31.htm

6.2 Mozilla Thunderbird

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes [15] für Windows, Linux und MacOS zur Verfügung. Linux Distributionen enthalten in der Regel Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung komfortabel installiert und aktualisiert werden.

6.2.1 Account erstellen

Nach dem ersten Start von Thunderbird führt ein Assistent durch die Schritte zur Einrichtung eines E-Mail Kontos. Nach Eingabe der E-Mail-Adresse sowie des Passwortes erkennt der Assistent die nötigen Einstellungen für den Mailserver oft automatisch. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden. Bei der Einrichtung des E-Mail Account sollten einige Punkte beachtet werden.

Die Grafik im Bild 6.1 zeigt den Weg einer E-Mail vom Sender zum Empfänger. In der Regel ist man nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der Firma.

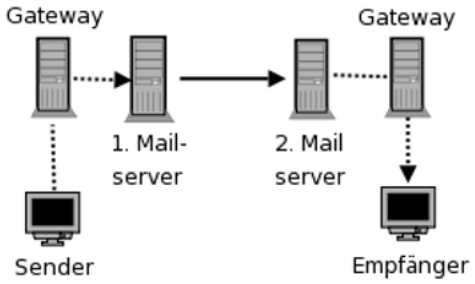


Abbildung 6.1: Der Weg einer E-Mail durch das Web

Der 1. Mailserver nimmt die E-Mail via SMTP entgegen und sendet sie an den 2. Mailserver. Hier liegt die E-Mail, bis der Empfänger sie via POP3 oder IMAP abruft und löscht. Die gestrichelten Verbindungen zu den Mailservern können mit SSL bzw. TLS kryptografisch gesichert werden. Das hat nichts mit einer Verschlüsselung des Inhalts der E-Mail zu tun. Es wird nur die Datenübertragung zum Mailserver verschlüsselt und es wird sichergestellt, dass man wirklich mit dem gewünschten Server verbunden ist. Aktuelle Versionen von Thunderbird aktivieren dieses Feature beim Einrichten eines Account standardmäßig.

Begrifferklärung: SMTP, POP3, IMAP und STARTTLS

Diese Abkürzungen sind für den Laien etwas verwirrend.

[15] https://www.mozilla.org/de/thunderbird/

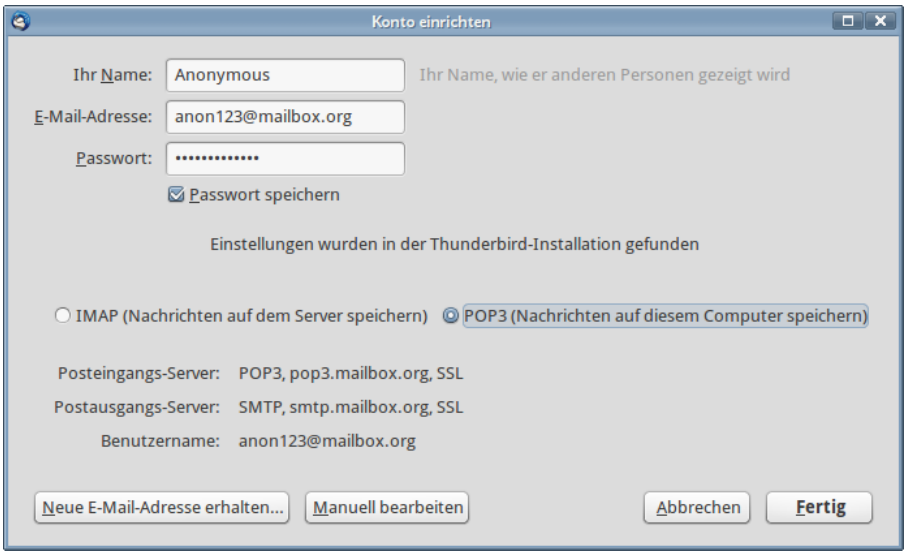


Abbildung 6.2: POP3-Account anlegen

SMTP: ist das Protokoll zum Versenden von E-Mails.

POP3: ist das Protokoll zum Herunterladen von empfangenen E-Mails auf den lokalen Rechner. Dabei werden die E-Mails auf dem Server sofort oder einige Tage später gelöscht.

Hinweis: bei POP3 wird nur der Ordner *Posteingang* vom Server geholt. Wenn man im Webinterface des Mailproviders weitere Ordner angelegt hat und mit Filtern E-Mails automatisch sortieren lässt, dann hat man mit POP3 keinen Zugriff auf diese Mails. Die automatische Sortierung muss in Thunderbird erfolgen.

IMAP: ist ein Kommunikationsprotokoll, um die empfangenen E-Mails auf dem Server zu verwalten und nur zum Lesen temporär herunter zu laden. Auch die versendeten E-Mails und Entwürfe werden bei der Nutzung von IMAP auf dem Mailserver des Providers gespeichert.

IMAP bietet damit die Möglichkeit, mit verschiedenen E-Mail Clients von unterschiedlichen Rechnern und Smartphones auf den Account zuzugreifen und stets Zugriff auf alle E-Mails zu haben. Die Möglichkeit des weltweiten Zugriffs auf seine Mails erkauft man sich aber mit Einschränkungen des Datenschutzes.

Die auf dem Server des Providers gespeicherten E-Mails unterliegen NICHT mehr dem Telekommunikationsgeheimnis nach Artikel 10 GG, wenn der Nutzer Gelegenheit hatte, sie zu löschen. Das BVerfG hat diese Rechtsauffassung 2009 in dem Urteil 2 BvR 902/06 bestätigt [16].

[16] https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-079.html

Mit der Reform der Telekommunikationsüberwachung im Dezember 2012 können Geheimdienste und Strafverfolge das Passwort für den Zugriff auf den Mail-Account ohne richterliche Prüfung vom Mail-Provider verlangen und damit Zugang zu dem Postfach erhalten. Es wäre unschön, wenn Sie dort die Kommunikation der letzten 5 Jahre vorfinden.

Wie einfach es ist, unverschlüsselte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde von T. Pritlove auf der re:publica 2007 demonstriert [17].

Alle brauchbaren Mail-Server bieten Möglichkeit der verschlüsselten Kommunikation zwischen Thunderbird und Mailserver. Diese Option ist in Thunderbird bei der Einrichtung eines neuen Kontos zu aktivieren. Der Assistent erledigt das in der Regel automatisch. In der Regel kann man bei der Transportverschlüsselung zwischen old-style SSL/TLS oder STARTTLS wählen.

SSL/TLS: Wenn man SSL/TLS verwendet, wird als erstes eine verschlüsselte Verbindung aufgebaut und danach beginnt die protokoll-spezifische Kommunikation. Es werden keine Daten unverschlüsselt übertragen.

STARTTLS: Wenn STARTTLS genutzt wird, beginnt die Kommunikation erst einmal unverschlüsselt. Der E-Mail Client wartet ab, ob der Mailserver in den Capabilities mit 250-STARTTLS eine Transportverschlüsselung anbietet. Erst dann erfolgt ein Aufbau der verschlüsselten Verbindung und der Client beginnt nochmal von vorn.

Eine SMTP-Verbindung wird mit STARTTLS wie folgt aufgebaut:

```
Client: unverschlüsselter Connect
Server: 220 smtp.server.tld Simple Mail Transfer Service Ready
Client: EHLO 192.168.23.44
Server: 250-smtp.server.tld
Server: 250-SIZE 100000000
Server: 250-AUTH LOGIN PLAIN
Server: 250-STARTTLS
Client: STARTTLS
Server: 220 go ahead
SSL/TLS Handshake zwischen Client und Server
Client (TLS-verschlüsselt): EHLO 192.168.23.44
```

Wie man sieht, können dabei unter Umständen auch private Daten unverschlüsselt gesendet werden. Bei SMTP wird im ersten EHLO Kommando die IP-Adresse oder der Hostname des Rechners aus dem internen Netz unverschlüsselt gesendet. Ein *Lauscher am Draht* kann damit u.U. den Mitarbeiter in einer Firma identifizieren.

[17] http://tim.geekheim.de/2007/04/24/netzwerksicherheit-auf-der-republica/

Bewusst oder unbewusst können auch Provider die sichere Übertragung deaktivieren und damit den Traffic mitlesen. Es wird einfach die Meldung des Mail-Servers 250-STARTTLS gefiltert und überschrieben. Scheinbar verfügen alle DSL-Provider über die Möglichkeit, dieses Feature bei Bedarf für einzelne Nutzer zu aktivieren[18]. Einige E-Mail Clients verwenden standardmäßig die Option *"STARTTLS wenn möglich"*. Diese Einstellung ist genau in dem Moment wirkungslos, wenn man es braucht, weil der Traffic beschnüffelt werden soll.

Das STARTTLS wurde als Erweiterung für bestehende Protokolle entwickelt, um TLS Verschlüsselung für unterschiedliche Domains mit unterschiedlichen Zertifikaten auf einem Server anbieten zu können. Es wurde nicht mit der Zielstellung entwickelt, die Sicherheit von SSL/TLS zu erhöhen. Man sollte sich nicht irritieren lassen und evtl. schlussfolgern, dass old-style SSL veraltet sein könnte.

Deshalb empfehlen wir die Nutzung von POP3 mit SSL/TLS (Bild 6.2).

Hinweis für Nutzer der Telekom-Router

Die aktuellen Versionen der DSL-Router, die von der Telekom bereitgestellt werden, haben ein Feature, um Spambogs das Versenden von E-Mails zu erschweren. SMTP-Verbindungen auf den Ports 25, 465 und 587 sind nur für eine Whitelist von Mail-Servern erlaubt. Die empfohlenen E-Mail Provider sind nicht alle in der standardmäßig aktivierten Whitelist enthalten.

In der Router Konfiguration kann man im Menüpunt *"Internet - Liste der sicheren E-Mail-Server"* das Feature abschalten oder den SMTP-Server des eigenen Providers hinzufügen.

Dieses Feature wird auch bei einem Update der Firmware älterer Telekom-Router aktiviert. Wenn man trotz korrekter Konfiguration in Thunderbird keine E-Mails mehr versenden kann, sollte man einen Blick in die Konfiguration des Routers werfen.

6.2.2 Sichere Optionen für SSL/TLS-Verschlüsselung

Die IETF hat im Mai 2015 die Richtlinien für den Einsatz von TLS-Verschlüsselung überarbeitet. Es wird ausschließlich der Einsatz von TLS 1.2 empfohlen. SSLv3 darf nicht mehr genutzt werden, TLS 1.0 und TLS 1.1 sollen nicht mehr genutzt. Außerdem gelten gemäß IETF RFC 7525 und BSI TR-03116-4 nur folgende Cipher für die TLS Verschlüsselung als sicher:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

[18] http://heise.de/-206233

Die E-Mail Provider können diese Empfehlungen nicht vollständig umsetzen, da es noch zuviele E-Mail Clients gibt, die diese sicheren Cipher (noch) nicht unterstützen. Um IETF-konforme, sichere SSL/TLS-Verschlüsselung für den Transport vom/zum Mail-Server zu erzwingen, kann man in Thunderbird selbst Hand anlegen in den *Erweiterten Einstellungen* die folgenden Optionen setzen:

- TLS v1.2 erzwingen:

```
security.tls.version.min =  3
```

- Alle nicht als sicher eingestuften Cipher deaktivieren, da bleibt bei Thunderbird nur zwei Cipher übrig:

```
security.ssl3.ecdhe_ecdsa_aes_128_gcm_sha256  = true
security.ssl3.ecdhe_rsa_aes_128_gcm_sha256    = true
security.ssl3.*                               = false
```

- Insecure Renegotiation verbieten:

```
security.ssl.require_safe_negotiation           = true
security.ssl.treat_unsafe_negotiation_as_broken = true
```

- Strenges Certifikate Pinning erwingen (z.B. für Add-on Updates):

```
security.cert_pinning.enforcement_level = 2
```

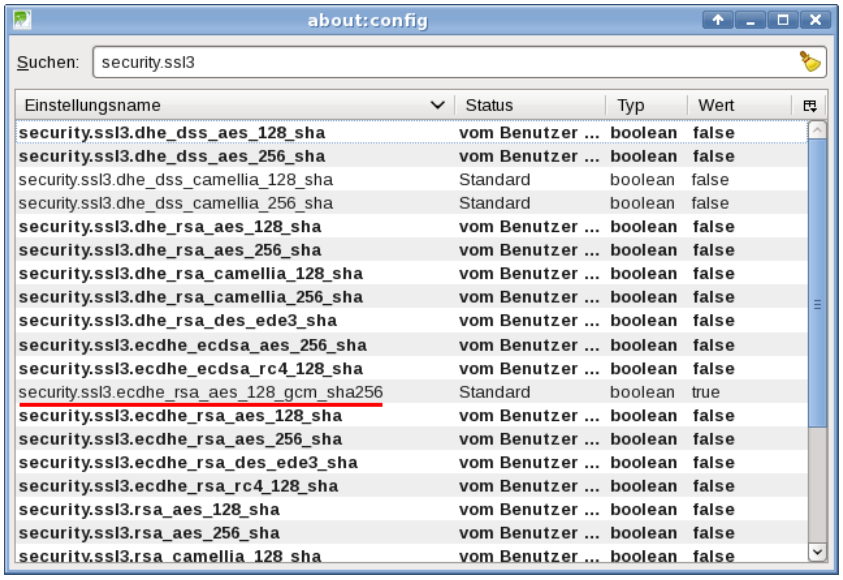


Abbildung 6.3: Konfiguration der SSL/TLS-Einstellungen für Thunderbird

Verbindungsprobleme

Wenn man die im Bild 6.4 gezeigte, schwer verständliche Fehlermeldung beim Abrufen oder Senden von E-Mails erhält, gibt es Probleme beim Aufbau einer sicheren Verbindung und man wechselt am besten den Mail-Provider. Oft bietet der Mail-Server keine *Secure Renegotiation* beim Aufbau der verschlüsselten Verbindung an. Das Problem wird seit 2009 als schwiegend eingestuft [19]. Ein Angreifer kann die Login Credentials (Username und Passwort) abschnorcheln ohne die Verschlüsselung knacken zu müssen. Tools zum Ausnutzen der Insecure Renegotiation für einen Angriff gibt es auch als OpenSource (z.B. dsniff).

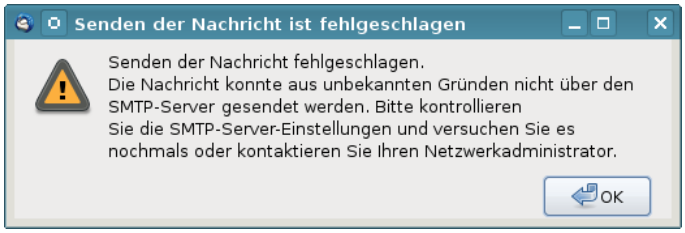


Abbildung 6.4: Fehlermeldung bei unsicherer Verbindung

SSL-Zertifikate mit DANE/TLSA prüfen (Linux)

IT-Sicherheitsforscher der EFF.org kamen bereits 2009 in einer wiss. Arbeit zu dem Schluss, dass Geheimdienste schwer erkennbare man-in-the-middle Angriffe mit gültigen SSL-Zertifikaten durchführen können. Dieser Angriff wird als *Lawful SSL Interception* bezeichnet. Firmen für Überwachungstechnik wie die deutsche Firma Utimaco bieten fertige Appliances dafür.

Gute E-Mail Provider veröffentlichen die SHA2-Hashes der SSL-Zertifikate für SMTP-, POP3- und IMAP-Server im DNS via DANE/TLSA Record, um diese Angriffe zu verhindern. Leider kann Thunderbird die SSL-Zertifikate (noch) nicht via DANE/TLSA überprüfen.

Linuxer können mit Komandozeilentools wie zB. *danetool* von GnuTLS prüfen, ob beim Aufbau einer verschlüsselten Verbindung zu den Mailservern das richtige Zertifikat verwendet wird oder ob ein Angriff mit einem Fake-Zertifikate erfolgt.

Als erstes ist GnuTLS zu installieren. Dabei muss man die Software selbst compilieren, da die Linux Distributionen das Paket *gnutls-bin* ohne DANE-Support erstellen. Dafür benötigt man auch einige Entwickler-Pakete, die man mit dem bevorzugten Paketmanager isnatllieren kann. Für Debian/Ubuntu funktioniert das folgende Kommando:

[19] https://www.verbraucher-sicher-online.de/news/fehlerhaftes-design-im-wichtigsten-verschluesselungsprotokoll-fuer-angriffe-nutzbar

```
> sudo aptitude install gcc make libgmp-dev libidn11-dev zlib1g-dev nettle-dev
                libunbound-dev libtasn1-6-dev
```

Nach dem Download der aktuellen Sourcen von der Webseite gnutls.org ist das Paket zu entpacken und mit dem üblichen Dreisatz zu installieren. Einige überflüssige Features kann man dabei deaktivieren:

```
> cd /usr/src/gnutls-3.4.x
> ./configure --disable-ocsp --disable-doc --disable-tests --without-p11-kit
> make
> sudo make install
> sudo ldconfig
```

Danach kann man mit dem Kommando *danetool –check* prüfen, ob das richtige Zertifikat für die Verschlüsselung verwendet werden würde, wenn man den SMTP, POP3 oder IMAP Server kontaktiert. Als Beispiel der Test eines SMTP Servers, wenn man den SMTP Server mit SSL-Verschlüsselung kontaktiert:

```
> danetool --check smtp.mailbox.org --port 465
Resolving 'smtp.mailbox.org'...
Obtaining certificate from '80.241.60.196:465'...
....
Verification: Certificate matches.
```

Wenn man STARTTLS Verschlüsselung im E-Mail Client nutzt, dann muss das Kommando ergänzt werden:

```
> danetool --check smtp.mailbox.org --port 587 --starttls-proto=smtp
Resolving 'smtp.mailbox.org'...
Obtaining certificate from '80.241.60.196:465'...
starttls: sending: STARTTLS
....
Querying DNS for smtp.mailbox.org (tcp:587)...
....
Verification: Certificate matches.
```

Und das gleiche nochmal für den POP3 Server mit SSL-Verschlüsselung:

```
> danetool --check pop3.mailbox.org --port 995
Resolving 'pop3.mailbox.org'...
Obtaining certificate from '80.241.60.199:995'...
....
Verification: Certificate matches.
```

Zum Abschluss ein Beispiel für einen IMAP Server mit STARTTLS-Verschlüsselung:

```
> danetool --check imap.mailbox.org --port 143 --starttls-proto=imap
Resolving 'imap.mailbox.org'...
Obtaining certificate from '80.241.60.199:143'...
starttls: sending: STARTTLS
Negotiating IMAP STARTTLS
```

```
starttls: sending: a CAPABILITY
....
Querying DNS for imap.mailbox.org (tcp:143)...
....
Verification: Certificate matches.
```

Es ist mühsam, vor dem Lesen oder Schreiben von E-Mails jedesmal ein Terminal zu öffnen, die seltsamen Befehle einzutippen und dann erst Thunderbird zu starten. Mit einem Startscript für Thunderbird oder jeden anderen E-Mail Client kann man den Test automatisieren und vor dem Start prüfen, ob die Zertifikate ok sind. Dabei der wird der Rückgabewert von *danetool* ausgewertet und eine Meldung angezeigt, wenn Fehler auftreten:

```
#!/bin/bash

# Check des SMTP Servers
danetool --check smtp.mailbox.org --port 465
if [ $? -ne 0 ]; then
   # SSL Zertifikatsfehler! Warnung und Abbruch
   zenity --error --text="DANE/TLSA Fehler bei SMTP Server!" --no-wrap
   exit 0
fi

# Check des POP3 Servers
danetool --check pop3.mailbox.org --port 995
if [ $? -ne 0 ]; then
   # SSL Zertifikatsfehler! Warnung und Abbruch
   zenity --error --text="DANE/TLSA Fehler bei POP3 Server!" --no-wrap
   exit 0
fi

# alles ok, Thunderbird kann starten
thunderbird
```

Das Prinzip ist einfach erkennbar und jeder Linuxer kann es selbst an die Mail Server von Posteo.de, Ownbay.net oder Kolab oder anpassen und ergänzen - oder?

Script kann man von meiner Webseite herunter laden und nach den nötigen Anpassungen z.B. nach *$HOME/.local/bin/* kopieren und als ausführbares Script kennzeichen:

```
> install -d $HOME/.local/bin
> cp Downloads/thunderbird_mit_danetest.sh $HOME/.local/bin
> chmod +x $HOME/.local/bin/thunderbird_mit_danetest.sh
```

Danach kann man in der Desktop Umgebung die Einstellungen für den bevorzugten E-Mail Client anpassen, einen Menüeintrag oder Starter auf dem Desktop erstellen, um das Script als E-Mail Client aufzurufen.

Einige kleine Vorschläge für Anpassungen:

- Im Beispiel habe ich das Tool *zenity* für die Anzeige der Warnung verwendet. Wer den KDE Desktop bevorzugt, möchte vielleicht lieber *kdialog* verwenden. Dann kann man die Zeilen für die Anzeige der Warnung (vor den *exit* Kommandos) austauschen:

  ```
  kdialog --error "DANE/TLSA Fehler bei SMTP Server!"
  ```

- Wenn man mehrere Profile in Thunderbrid verwendet (z.B. *default* und *anonym mit JonDo/Tor*), dann möchte man am Ende mit dem letzten Kommando gleich das passende Profil starten. Das funktioniert mit folgender Option für Thunderbird/Icedove:

  ```
  thunderbird -P "r3wq6m51.default"
  ```

  Der Name des Profils ist selbst anzupassen. Wenn man einen anderen E-Mail Client verwendet, ist der letzte Befehl zu ersetzen (z.B. kmail, evolution....).

- Bei der Verwendung von Tor Onion Router als Anonymisierungsdienst ist der Test wenig aussagekräftig, weil die Route durch das Tor Netzwerk häufig wechselt. Wenn man 20min nach dem Test eine neue E-Mail endlich abschickt, dann wird eine andere Route mit einem anderen Tor Exit Node verwendet und das Testergebnis ist hinfällig.

6.2.3 Sichere Konfiguration des E-Mail Client

Einige Hinweise für die sichere und unbeobachtete Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- Mit der Verwendung von HTML in E-Mails steht dem Absender ein ganzes Bestiarium von Möglichkeiten zur Beobachtung des Nutzers zur Verfügung: HTML-Wanzen, Java Applets, JavaScript, Cookies usw. Die Firma ReadNotify beispielsweise nutzt diese Möglichkeiten, um E-Mails für die Beobachtung des Empfängers zu präparieren (User-Tracking). Der *E-Mail Privacy Test*[20] demonstriert viele Trackingmöglichkeiten.

  Standardmäßig blockiert Thunderbird alle Trackingelemente und auch Spam Mails in der HTML Ansicht. Trotzdem empfehle ich, E-Mails als Plain Text zu lesen. Die Option findet man im Menüpunkt *Ansicht -> Nachrichtentext* (siehe Bild 6.5).

- Die Option *Anhänge eingebunden anzeigen* im Menü *Ansicht* sollte man ebenfalls deaktivieren, um gefährliche Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen. Der alte Trick mit einem Virus in der E-Mail wird noch immer genutzt, insbesondere wenn man ein Opfer gezielt angreifen will, um den Rechner mit einem Trojaner zu infizieren.

[20] https://emailprivacytester.com

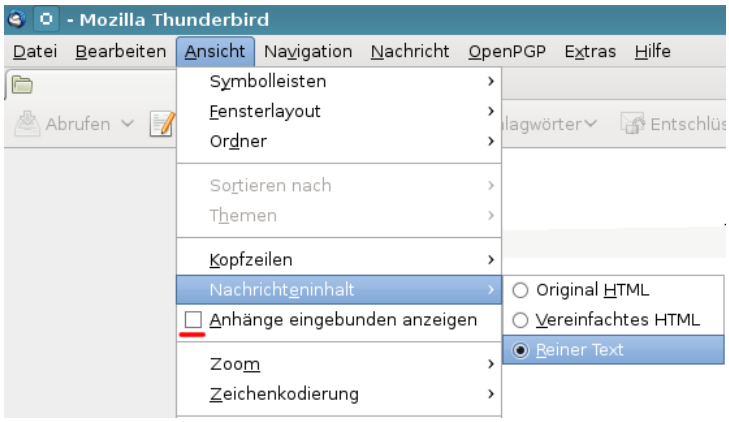


Abbildung 6.5: E-Mails als reinen Text darstellen

- Es ist nicht immer möglich, E-Mails als Plain Text zu lesen. Viele Newsletter sind nur als HTML-Mail lesbar, eBay verwendet ausschließlich HTML-Mails für Benachrichtigungen usw. In der Regel enthalten diese HTML-only Mails mehrere Trackingelemente.

  Um diese E-Mails trotzdem lesen zu können (wenn auch nicht in voller Schönheit), kann man die Darstellung *Vereinfachtes HTML* nutzen. Außerdem können folgende Features in den *Erweiterten Einstellungen* deaktiviert werden, die jedoch nur für die Darstellung von *Orginal HTML* relevant sind:

```
javascript.enabled                    =  false
network.cookie.cookieBehavior         =  2
dom.storage.enabled                   =  false
dom.indexedDB.enabled                 =  false
geo.enabled                           =  false
webgl.disabled                        =  true
layout.css.visited_links_enabled      =  false
gfx.downloadable_fonts.enabled        =  false
network.http.sendRefererHeader        =  0
network.http.use-cache                =  false
```

- Alle Bilder in HTML-Mails, die von einem externen Server geladen werden, können direkt mit der E-Mail Adresse des Empfängers verknüpft sein. Anhand der Logdaten kann der Absender erkennen, wann und wo die E-Mail gelesen wurde. Einige Newsletter verwenden auch HTML-Wanzen. Im Newsletter von Paysafecard findet man beispielsweise ganz unten eine kleine 1x1-Pixel Wanze, die offenbar mit einer individuellen, nutzerspezifischen URL von einem Trackingservice geladen wird:

```
<IMG src="http://links.mkt3907.com/open/log/43.../1/0">
```

Easyjet.com (ein Billigflieger) kann offenbar die Aufrufe seiner Newsletter selbst zählen und auswerten. In den E-Mails mit Informationen zu gebuchten Flügen findet man folgende kleine Wanze am Ende der Mail:

```
<IMG src="http://mail.easyjet.com/log/bEAS001/mH9..."
     height=0 width=0 border=0>
```

Um Tracking mit Bildern und HTML-Wanzen zu verhindern, kann man in den *Erweiterten Einstellungen* das Laden externer Bilder blockieren:

```
permissions.default.image  =  2
```

Auch andere Medienformate können von einem externen Server geladen und als Wanzen genutzt werden. Einen deartigen Einsatz von Audio- oder Videodateien habe ich bisher nicht gefunden, aber technisch wäre es möglich. Man kann das Laden von Videos und Audiodateien mit folgenden Parametern unterbinden:

```
media.webm.enabled  =  false
media.wave.enabled  =  false
media.ogg.enabled   =  false
```

Die Links in HTML-Mails führen oft nicht direkt zum Ziel sondern werden ebenfalls über einen Trackingservice geleitet, der jeden Aufruf des Link individuell für jede Empfängeradresse protokollieren kann. Als Bespiel soll ein Link aus dem Paysafecard Newsletter dienen, der zu einem Gewinnspiel bei Paysafecard führen soll:

```
<a href="http://links.mkt3907.com/ctt?kn=28&ms=3N...">
Gewinne Preise im Wert von 10.000 Euro</a>
```

Diesem Tracking kann man nur entgehen, wenn man diese Links in HTML-Mails nicht aufzuruft! Der Trackingservice hat die Möglichkeit, Logdaten von verschiedenen E-Mails zu verknüpfen und evtl. auch das Surfverhalten einzubeziehen. Wichtige Informationen findet man auch auf der Webseite des Absenders.

- Im SMTP-Dialog mit dem Mailserver beim Versenden einer E-Mail sendet Thunderbird im EHLO Kommando standardmäßig die lokale IP-Adresse aus dem internen Netzwerk:

  ```
  SSL/TLS Handshake zwischen Client und Server
  Client: EHLO 192.168.23.44
  ```

  Viele Mailserver vermerken diese lokale IP-Adresse aus dem EHLO Kommando im ersten Received Header der E-Mail zusammen mit der externen IP-Adresse, die der Mailserver sieht, und teilen sie damit auch Dritten mit:

  ```
  Received: from cefige3264.dynamic.kabel-deutschland.de
  ([188.192.92.109] helo=[192.168.23.44]) by smtp.server.tld
  ```

Um zu vermeiden, dass diese Information veröffentlicht wird, kann in den *Erweiterten Einstellungen* folgenden Wert als String Variable neu anlegen und einen Fake definieren:

```
mail.smtpserver.default.hello_argument = [127.0.0.1]
```

Anmerkung: Privacy-freundliche E-Mail Provider entfernen den ersten Received Header vollständig, da er nicht nur die lokale IP-Adresse aus dem internen Netzwerk enthält, sondern auch die externe IP-Adresse, die Hinweise auf den Aufenthaltsort des Absenders liefert und von Datensammlern mit dem Surfprofil verknüpft werden kann.

- Die *extension blocklist* kann Mozilla nutzen, um einzelne Add-ons in Thunderbird zu deaktivieren. Es ist praktisch ein kill switch für Thunderbird Add-ons. Beim Aktualisieren der Blockliste werden außerdem detaillierte Informationen an Mozilla übertragen.

  Ich mag es nicht, wenn jemand irgendetwas remote auf meinem Rechner deaktiviert oder deaktivieren könnte. In den *Erweiterten Einstellungen* kann man das Feature abschalten:

  ```
  extensions.blocklist.enabled = false
  ```

  Thunderbird kontaktiert täglich den AMO-Server von Mozilla und sendet eine genaue Liste der installierten Add-ons. Als Antwort sendet der Server Statusupdates für die installierten Add-ons. Diese Funktion ist unabhägig vom Update Check für Add-ons, es ist nur eine zusätzliche Datensammlung von Mozilla. In den erweiterten einstellungen kann amn dieses Feature abschalten:

  ```
  extensions.getAddons.cache.enabled = false
  ```

- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server können mit einem Masterpasswort geschützt werden.

6.2.4 Datenverluste vermeiden

Die folgenden Hinweise wurden von den Mozilla-Entwicklern erarbeitet, um den Nutzer bestmöglich vor Datenverlusten zu schützen:

- Das Antiviren-Programm ist so einzustellen, dass es den Profilordner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.

- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.

- Die Ordner sollten regelmäßig komprimiert werden, um gelöschte E-Mails engültig aus der MBOX zu entfernen und den Speicherplatz freizugeben.

  - In den Einstellungen in der Sektion *Erweitert* kann man eine automatische Komprimierung konfigurieren, sobald x MB Speicherplatz dadurch frei werden. Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.
  - Alternativ kann man mit der rechten Maustaste auf einen Ordner zu klicken und der Punkt *Komprimieren* wählen. Während des Komprimierens sollten keine anderen Aktionen in Thunderbird ausgeführt werden.

- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*, unter Linux ist *$HOME/.thunderbird* zu sichern.

6.2.5 Wörterbücher installieren

Nach der Installation von Thunderbird sind keine Wörterbücher für die Rechtschreibkontrolle vorhanden. Die Wörterbücher müssen zusätzlich installiert werden, wenn man auf das Feature nicht verzichten möchte. Nach dem Download der Wörterbücher [21] ist Thunderbird als zu starten. Der Menüpunkt *Extras -> Add-ons* öffnet den Dialog für die Verwaltung. Wenn man oben rechts auf das kleine Werkzeugsymbol klickt (Bild 6.6, kann man die Dateien mit den Wörterbüchern als Add-on installieren.

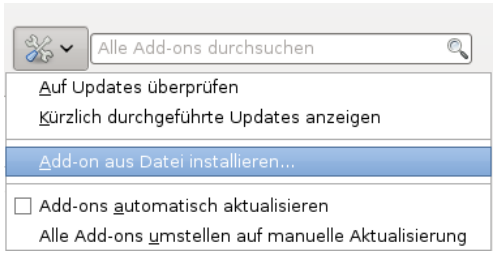


Abbildung 6.6: Wörterbücher in der Add-on Verwaltung installieren

Danach kann man in den Einstellungen von Thunderbird die Rechtschreibprüfung aktivieren und die bevorzugte Sprache auswählen. Die Auswahl der Sprache kann man beim Schreiben einer Mail jederzeit ändern.

6.2.6 User-Agent Kennung modifizieren

Ich habe gelesen, dass es böse Buben geben soll, die via Internet ihre Software auf fremden Rechnern installieren möchten. Das Versenden von böstigen E-Mail Attachements via E-Mail ist Bestandteil jeder Werkzeugkiste für Angreifer.

[21] https://addons.mozilla.org/de/thunderbird/language-tools/

- Der Bundestrojaner, den das BKA zu Spionage einsetzt, wird unter anderem via E-Mail auf den Rechner der Zielperson transportiert, wie die Tagesschau berichtete.[22]
- 2010 wurde Google bzw. von US-Regierungsvertretern genutzte GMail Accounts von chinesischen Hackern angegriffen. Auch dabei wurden E-Mails mit bösartigen Attachements verwendet, wie Google in einem Statement berichtete.[23]
- Auch als unbescholtener Bürger kann man zufällig Target für einen gezielten Angriff werden. Beispielsweise hackt die NSA gezielt die Rechner von Sysadmins, um über diesen Weg Zugang zu technischer Infrastruktur zu bekommen.[24]

Voraussetzung für diese gezielten Angriffe ist die Kenntnis der vom Opfer zum Lesen von E-Mails verwendete Software. Dann kann ein Angreifer gezielt für diesen E-Mail Client oder Browser einen Exploit auswählen, der unauffällig funktioniert. Genau wie jeder Webbrowser sendet auch Thunderbird eine User-Agent-Kennung im Header jeder E-Mail, die Auskunft über die genutzte Programmversion und das Betriebssystem liefert. Das folgende (veraltete) Beispiel stammt aus der Mail eines Unbekannten:

```
...
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0)
            Gecko/20100101 Thunderbird/38.2.0
X-Enigmail-Version: 1.8.1
...

------- BEGIN PGP MESSAGE -------
Version: GnuPG v1.4.12 (GNU/Linux)
...
```

Aha, er nutzt also Thunderbird in der Version 38.2.0 unter Windows 7 (64 Bit), hat das Enigmail Add-on Version 1.8.1 installiert und verwendet die GnuPG-Version 1.4.12.

Einige privacy-freundliche Mailprovider wie mailbox.org und Mail.de reinigen die Mails für Ihre Kunden und löschen die User-Agent Kennung aus dem E-Mail Header. Wenn man einen Account bei einem anderen Mailprovider hat, dann muss man sich selbst kümmern.

Die User-Agent-Kennung kann in den erweiterten Einstellungen modifiziert werden. Im Einstellungs-Dialog findet man in der Sektion *Erweitert* den Reiter *Allgemein*. Ein Klick auf den Button Konfiguration bearbeiten öffnet eine Liste aller Optionen.

Hier fügt man die neue String-Variable **general.useragent.override** als neuen Wert ein, indem man mit der rechten Maustaste auf einen freien Bereich

[22] https://www.tagesschau.de/inland/meldung490134.html
[23] https://googleblog.blogspot.de/2010/01/new-approach-to-china.html
[24] https://theintercept.com/2014/03/20/inside-nsa-secret-efforts-hunt-hack-system-administrators/

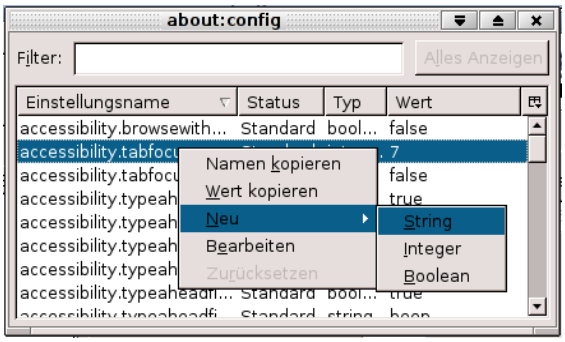


Abbildung 6.7: Neue Config-Variable anlegen

klickt und im Kontext-Menü den Punkt *Neu - String* wählt.Als Wert für diese Variable wird eine leere Zeichenkette eingesetzt. Damit sendet Thunderbird keine Kennung mehr. Nachteile sind nicht erkennbar.

Wer das Add-on Enigmail für die Verschlüsselung nutzt, sollte dem Add-on die Geschwätzigkeit abgewöhnen und die Ausgabe von Versionen im Header deaktivieren. Anderenfalls kann ein Schnüffler anhand einer signierten oder verschlüsselten E-Mail Schlussfolgerungen über die verwendete Software ableiten. Folgende Parameter sind in den erweiterten Einstellungen zu setzen:

```
extensions.enigmail.addHeaders            =  false
extensions.enigmail.useDefaultComment     =  true
extensions.enigmail.agentAdditionalParam  =  --no-emit-version
```

Die Kalender- und Aufgabenverwaltung *Lightning* hängt die eigene Version noch zusätzlich an die User-Agent Kennung an. Wenn man dieses Add-on nutzt, muss man in den erweiterten Einstellungen außerdem folgende Variable auf einen leeren String setzen:

```
calendar.useragent.extra = ""
```

6.2.7 Spam-Filter aktivieren

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter kann man in Account Einstellungen unter *Junk-Filter* aktivieren, wenn der E-Mail Provider keinen guten Spam-Filter einsetzt.

(Ich nutze lieber einen guten E-Mail Provider und brauche daher diesen Spam-Filter seit längerer Zeit nicht mehr.)

6.2.8 Spam vermeiden

Die E-Mail Adresse ist ein wichtiges Identitätsmerkmal. Datensammler wie Rapleaf verwenden sie als ein Hauptmerkmal für die Identifikation, um

darauf aufbauend Profile zu erstellen. Stichproben im Internet Traffic weisen einen hohen Anteil von Suchanfragen nach Informationen zu den Inhabern von E-Mail Adressen aus.

Man muss die eigene E-Mail Adresse nicht bei jeder Gelegenheit im Web angeben, wenn irgendwo eine E-Mail Adresse verlangt wird (bei der Registrierung in Foren, einfachen Blog Postings usw). Um die eigene E-Mail Adresse nicht zu kompromittieren und trotzdem diese Angebote zu nutzen, kann man E-Mail Aliases, Wegwerf-Adressen oder temporäre E-Mail Adressen nutzen.

E-Mail Aliases nutzen

Jeder brauchbare E-Mail Provider bietet die Möglichkeit, Aliases für einen E-Mail Account anzulegen. Man kann im Webinterface in den Konfigurationseinstellungen einen oder mehrere Aliases für den Account erstellen, diese Adressen für die Kommunikation mit bestimmten Zweck (z.B für Hotel Reservierung oder Flug Buchung) für eine begrenzte Zeit nutzen und dann löschen. Konkrete Anleitungen findet man in den FAQ oder der Online Hilfe des Mail Providers.

Die Verwendung von E-Mail Aliases hat gegenüber temporären E-Mail Adressen und Wegwerf-Adressen einige Vorteile:

- E-Mail Aliases können auch als Absender zum Senden von E-Mails verwendet werden. Das ist z.B. ein Vorteil, wenn man nach der Registrierung eines Accounts den Support des Anbiters kontaktieren muss. Mit temporären Adressen kann man in der Regel nur Nachrichten empfangen.
- E-Mail Aliases werden nicht gesperrt. In vielen Diskussionsforen (z.B. bei Zeit.de) sind E-Mail Adressen von Temp.-Mail Anbietern für die Registrierung von Accounts gesperrt.
- Gute E-Mail Provider haben ein sichere TLS Transportverschlüsselung für ihre Mailserver. Bei den Anbietern temporärer E-Mail Adressen werden die Mails in der Regel ohne oder mit schlechter TLS Verschlüsselung durch das Internet gesendet und können von Dritten (z.B. vom BND in Rahmen der Fernmeldeaufklärung) problemlos mitgelesen werden.

E-Mail Adress-Erweiterungen

Bei vielen E-Mail Providern Mailbox.org, Runbox, Gmail, Yahoo! Mail Plus, Apple's iCloud, Outlook.com oder FastMail kann man E-Mail Adress-Erweiterungen nutzen. Wenn man die E-Mail Adresse *name@provider.tld* als Account oder E-Mail Alias registriert hat, kann man beliebig viele Adresse nach dem Muster *name+extension@provider.tld* zum Empfang verwenden. Es ist ein Standardfeature des MTA Postfix und kann auch auf eigenen Mailservern einfach aktiviert werden.

Einige E-Mail Provider bewerben dieses Feature als Spamschutz. Nach unserer Meinung ist der Wert als Spamschutz aber sehr gering. Jeder, der sich ein bisschen mehr mit E-Mail Features beschäftigt hat (und davon kann man

bei Datensammlern ausgehen), kennt das Feature und kann die Erweiterungen leicht ausfiltern. Der Vorteil von E-Mail Adress-Erweiterungen liegt eher in der einfach konfigurierbaren, automatischen Sortierung eingehender Nachrichten und nicht beim Spamschutz.

AnonBox des CCC

Bei der AnonBox.net des CCC [25] kann ein E-Mail Account für den Empfang von einer Nachricht erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig und nicht verlängerbar. Eingehende Nachrichten kann man nur im Webinterface lesen und sie werden nach dem Abrufen gelöscht. Sie können nur 1x gelesen werden! Zusammen mit der E-Mail wird auch der Account gelöscht. Man kann praktisch nur eine Mail empfangen.

Beim Erzeugen einer E-Mail Adresse erhält man einen Link, unter dem man ankommende Mails lesen kann. Wenn noch nichts angekommen ist, dann bleibt die Seite leer. Der Link ist als Lesezeichen zu speichern, wenn man später nochmal nachschauen möchte.

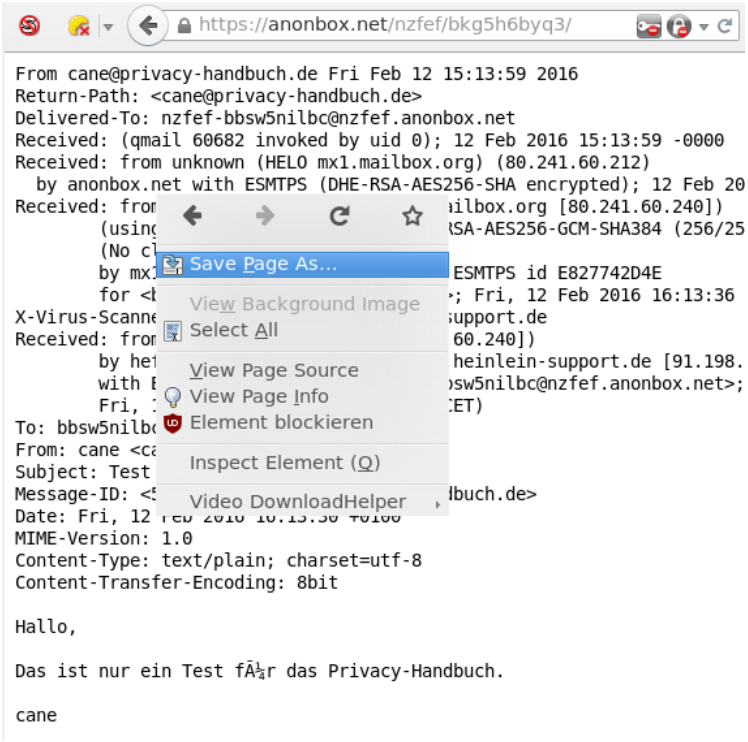


Abbildung 6.8: E-Mail im Web-GUI der AnonBox.net als Datei speichern

Eine empfangene E-Mail wird im Quelltext dargestellt. Wer aus dem Konvolut nicht schlau wird, kann mit de rechten Maustaste in die Textwüste

[25] https://anonbox.net

klicken und als Datei speichern, wie in Bild 6.8 gezeigt. Die Datei ist mit der Endung **.eml** zu speichern und kann dann in einem E-Mail Client wie z.B. Mozilla Thunderbird geöffnet werden (Bild 6.9).

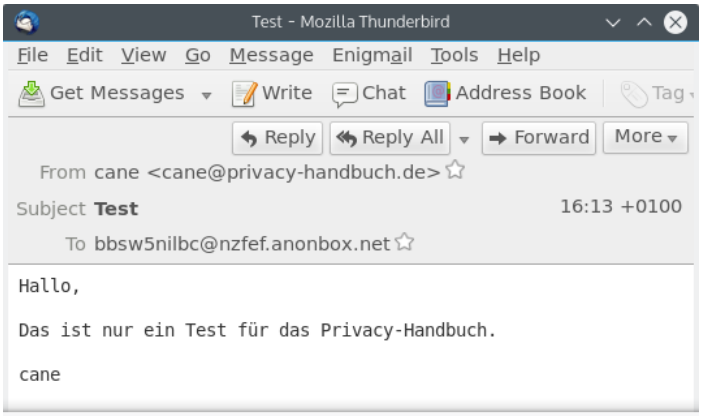


Abbildung 6.9: E-Mail aus AnonBox.net in Thunderbird geöffnet

Sicherheit der SSL/TLS Transportverschlüsselung bei AnonBox.net:

- Die SSL-Konfiguration des Webservers von AnonBox.net ist auf dem aktuellen Stand der Technik mit Forward Secrecy und starken DH-Parametern. Es wird ein Zertifikat von Let's Encrypt verwendet, das von allen Browsern anerkannt wird.

Wegwerf-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert und auch kein Erstellen der Adresse vor der Nutzung. E-Mail Adressen der Form *pittiplatsch@trash-mail.com* oder *pittiplatsch@weg-werf-email.de* kann man überall und ohne Vorbereitung unbekümmert angeben. Das Postfach ist unbegrenzt gültig.

In einem Webformular auf der Seite des Betreibers findet man später alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es in der Regel keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen und löschen. Wenn eine Wegwerf-Adresse für die Registrierung eines Account genutzt wurde, könnte ein Angreifer problemlos die Passwort Recovery Funktion nutzen!

Nachrichten werden nach 6-12h automatisch gelöscht. Man muss also regelmäßig den Posteingang prüfen, wenn man eine Wegwerf-Adresse nutzt.

Liste einiger Anbieter (unvollständig):

- https://discard.email (SSL-Verschlüsselung für Webserver aber nicht für Mailserver, Passwortschutz, E-Mail schreiben möglich, Session-Cookies und Javascript erforderlich)
- https://www.trash-mail.com (HTTPS, Cookies und Javascript freigeben, Schreiben von E-Mails möglich)
- https://www.guerrillamail.com (HTTPS, Cookies und Javascript freigeben, Schreiben von E-Mails möglich)
- http://crapmail.dk (Antwort schreiben möglich, Cookies freigeben)
- http://vsimcard.com/trashmails.php (bietet auch Wegwerf-SMS Nummern)
- http://www.7mail7.com (Cookies und Javascript freigeben, RSS-Feed für Inbox)
- http://www.mailcatch.com (keine Cookies oder Javascript nötig, E-Mails können gelöscht werden)
- http://www.mailinator.com/ (Javascript nötig freigeben, E-Mails können gelöscht werden)

In der Regel speichern diese Anbieter die Informationen über eingehende E-Mails sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. Es handelt sich dabei nicht Anonymisierungsdienste.

Temporäre Adressen

Im Gegensatz zu Wegwerf-E-Mail-Adressen muss man eine temporäre E-Mail Adresse zuerst auf der Webseiten des Anbieter erstellen, die dann für 10min bis zu mehreren Stunden gültig ist. Erst danach kann diese Mail-Adresse verwendet werden. Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse im Browser mehrfach verlängert werden.

Um eine temporäre E-Mail Adresse für die Anmeldung in einem Forum o.ä. zu nutzen, öffnet man als erstes eine der oben angegebenen Webseiten in einem neuen Browser-Tab. Session-Cookies sind für diese Website freizugeben, mit Javascript sind die Webseiten oft besser bedienbar. Nachdem man eine neue temporäre Mail-Adresse erstellt hat, überträgt man sie mit Copy & Paste in das Anmeldeformular uns schickt das Formular ab. Dann wechselt man wieder zu dem Browser-Tab der temporären Mailadresse und wartet auf die eingehende Bestätigungsmail. In der Regel einhält diese Mail einen Link zur Verifikation. Auf den Link klicken - fertig. Wenn der Browser-Tab mit der temporäre E-Mail Adresse geschlossen wurde, hat man keine Möglichkeit mehr, ankommende Mails für diese Adresse zu lesen.

Die folgenden Anbieter erlauben nur zufällig erstellter E-Mail Adressen. Die Verwendung dieser Adressen für die Registrierung von Accounts ist sicherer, da ein Angreifer die Passwort Recovery Funktion des Webdienstes nicht

nutzen kann, um sich ein neues Passwort zuschicken zu lassen und den Account zu übernehmen:

- https://temp-mail.ru (2h, HTTPS, Cookies und Javascript freigeben, russsiches GUI)
- www.10minutemail.com (10min gültig, verlängerbar)
- http://www.10minutemail.com/ (10min gültig, verlängerbar, Cookies und Javascript freigeben)
- http://tmpeml.info (60min gültig, Cookies freigeben)
- http://disposable.pingfu.net (60min gültig, Javascript freigeben)
- http://getairmail.com (24h gültig, Cookies und Javascript freigeben)

Bei den folgenden Anbieter kann man neben zufällig generierten E-Mail Adressen auch selbst definierte E-Mail Adresse nutzen. Man kann damit einen bestimmten E-Mail Account mehrfach verwenden. Das ist für einige Anwendungsfälle ein Vorteil, manchmal eher ein Nachteil:

- http://www.tempmailer.de (60min gültig, Session-Cookies freigeben)
- http://www.squizzy.de (60min gültig, Session-Cookies freigeben)
- http://dontmail.net (24h, Cookies und Javascript freigeben)
- http://www.migmail.net (24h, Cookies und Javascript freigeben)

Firefox Add-on Bloody Vikings

Die Firefox Add-ons *Bloody Vikings* [26] und der JonDoFox vereinfacht die Nutzung von Wegwerfadressen. Nach der Installation von der Webseite kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden.

In Zukunft kann man in jedem Anmeldeformular mit der rechten Maustaste auf das Eingabefeld der E-Mail Adresse klicken und aus dem Kontextmenü den Punkt *Bloody Vikings* wählen. Es wird in einem neuen Browser Tab die Webseite des Anbieters geöffnet und die temporäre E-Mail Adresse in das Formularfeld eingetragen. Nach dem Absenden des Anmeldeformular wechselt man in den neu geöffneten Browser Tab und wartet auf die Bestätigungsmail.

6.2.9 RSS-Feeds

RSS-Feeds bieten die Möglichkeiten, sich schnell über Neuigkeiten in häufig gelesenen Blogs zu informieren ohne die Webseiten einzeln abklappern zu müssen. Thunderbird enthält einen RSS-Reader, den man dafür nutzen kann.

Um mehrere interessante RSS-Feeds zu sammeln, erstellt man in der *Konten Verwaltung* ein neues Konto und wählt den Typ *Anderes Konto hinzufügen....*

[26] https://addons.mozilla.org/de/firefox/addon/bloody-vikings

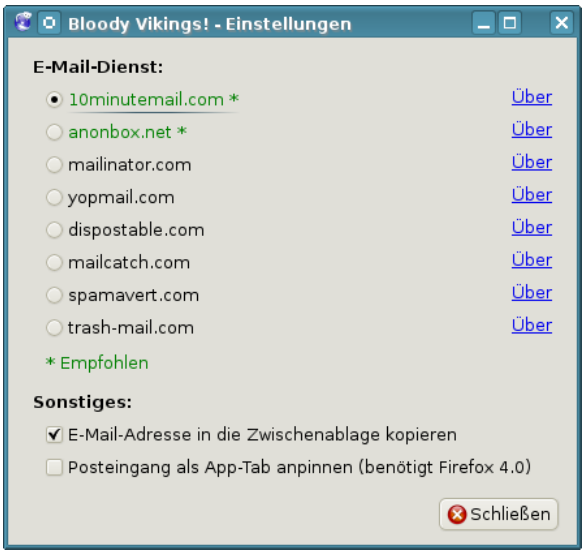


Abbildung 6.10: Bloody Vikings konfigurieren

Im zweiten Schritt wählt man den Typ *Blogs und RSS-Feeds* und danach eine beliebige Kontenbezeichnung.

In den Einstellungen für das RSS-Feed Konto kann man festlegen, in welchem Intervall die Feeds abgerufen werden sollen und ob die RSS-Feeds beim Start von Thunderbird aktualisiert werden sollen. Danach kann man die *Abonnements verwalten* und die Adressen der RSS-Feeds hinzufügen. Man kopiert die URL des RSS-Feeds von der Webseite des Blogs in das Feld für die Feed URL und klickt auf den Button *Hinzufügen* wie im Bild 6.11 dargestellt.

Die Neuigkeiten aus den Blogs kann man zukünftig wie E-Mails lesen. Dabei kann man eine simple Textanzeige wählen oder die Ansicht als Webseite. Wer die Ansicht als Webseite bevorzugt, sollte Javascript, Cookies und andere Tracking Elemente deaktivieren. Zum Kommentieren muss man allerdings die Webseite des Blogs im Browser aufrufen.

6.2.10 Filelink

Seit Version 13.0 bietet Thunderbird die Möglichkeit, große Dateianhänge bei einem Filehoster hochzuladen und dem Empfänger nur den Link zum Download per E-Mail zu senden. In der Version 16.0 unterstützt Thunderbird

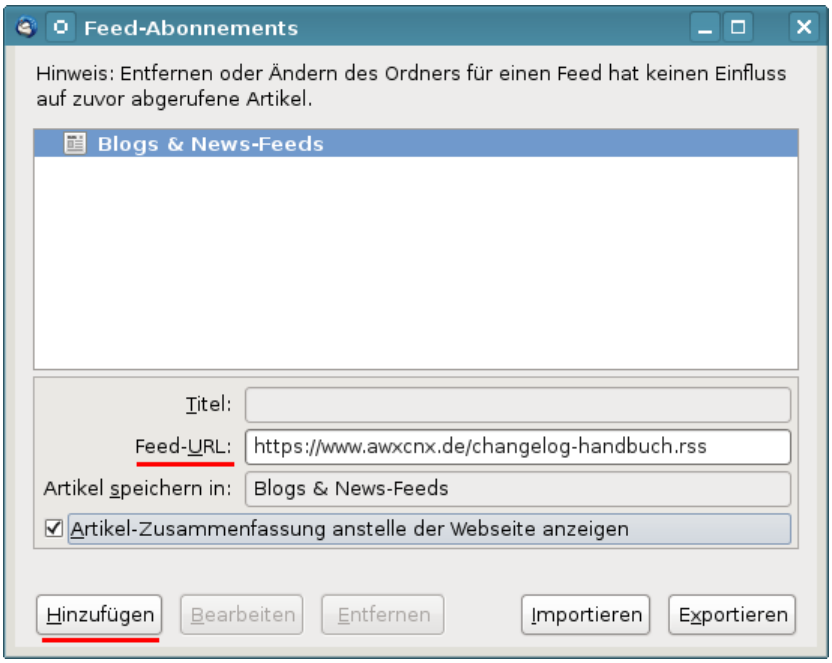


Abbildung 6.11: RSS-Feed hinzufügen

die Filehoster YouSendIt[27] und Box.net[28] sowie Ubuntu One.

Ich kann dieses Feature nicht empfehlen.

1. YouSendIt protokolliert alle Aktivitäten und die Protokolle werden für drei Jahre gespeichert:

   > *YouSendIt will retain the Log Data collected from you in its active, internal company databases for up to six months, at which point it will migrate such Log Data to its offline archival systems, where YouSendIt will retain the Log Data for a period of three years.*

2. Die bei einem Cloud-Service gespeicherten Dateianhänge unterliegen nicht dem besonderen Schutz des Post- und Fernmeldegeheimnisses.

3. Außerdem ist das Filelink nicht in die E-Mail Verschlüsselung integriert. Auch wenn man eine verschlüsselte E-Mail schreibt, werden die Uploads unverschlüsselt auf dem Server abgelegt. Man muss sich selbst um die Verschlüsselung der Dateien kümmern. Dann kann man sie auch gleich selbst zu einem 1-Click-Hoster hochladen.

Um nicht ständig mit der Frage belästigt zu werden, ob man einen großen Dateianhang bei einem Cloude-Anbieter speichern möchte, kann man das Feature in den Einstellungen deaktivieren.

[27] https://www.yousendit.com
[28] https://www.box.com/

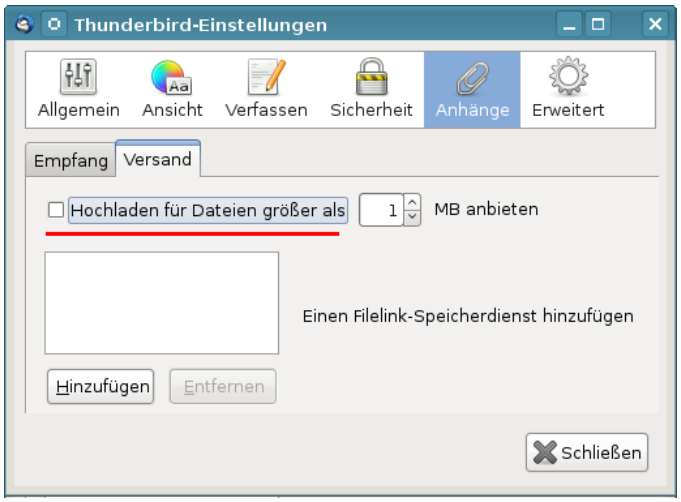


Abbildung 6.12: Filelink deaktivieren

6.3 Private Note

E-Mails werden auf dem Weg durch das Netz an vielen Stellen mitgelesen und ausgewertet. Ein Postgeheimnis existiert praktisch nicht. Kommerzielle Datensammler wie Google und Yahoo scannen alle Mails, die sie in die Finger bekommen. Geheimdienste wie NSA, SSSI, FRA oder BND haben Monitoringprogramme für den E-Mail Verkehr.

Gelegentlich möchte man aber nicht, das eine vertrauliche Nachricht von Dritten gelesen wird. Verschlüsselung wäre eine naheliegende Lösung. Das ist aber nur möglich, wenn Absender und Empfänger über die nötige Kompetenz verfügen.

Als Alternative kann man *PrivNote*[29] der Firma *insophia* nutzen. Man schreibt die Nachricht auf der Webseite des Anbieters und klickt auf den Button *Create Note*. Javascript muss dafür frMan schreibt die Nachricht auf der Webseite des Anbieters. Javascript muss dafür freigegeben werden. In den Optionen kann man festlegen, wann die Nachricht gelöscht werden soll, man kann zusätzlich ein Passwort für das Lesen setzen und eine E-Mail bekommen, wenn die Nachricht gelöscht wird.

Das zusätzliche Passwort ist nur sinnvoll, wenn es über einen unabhängigen Kanal zum Empfänger übertragen wird. Man könnte z.B. bei einem Treffen ein Passwort vereinbaren und dieses Passwort dann nutzen, bis man ein neues Passwort austauscht. Das Passwort könnte man mit jeder Nachricht ändern, so dass die aktuelle Nachricht immer das Passwort für die nächste Nachricht enthält. Man kann es beliebig kompliziert gestalten, solange beide Seiten den Überblick behalten. Es ist aber nicht sinnvoll, ein Passwort zusammen mit

[29] https://privnote.com

dem Link zum Lesen der Nachricht in der gleichen E-Mail zu schicken, das ist Bullshit.

Wenn man auf den Button *Create note* klickt, wird ein Link generiert, unter dem man die Nachricht EINMALIG abrufen kann. Die Nachricht wird im Browser verschlüsselt auf dem Server gespeichert und nur der Link enthält den Key, um die Daten zu entschlüsseln.

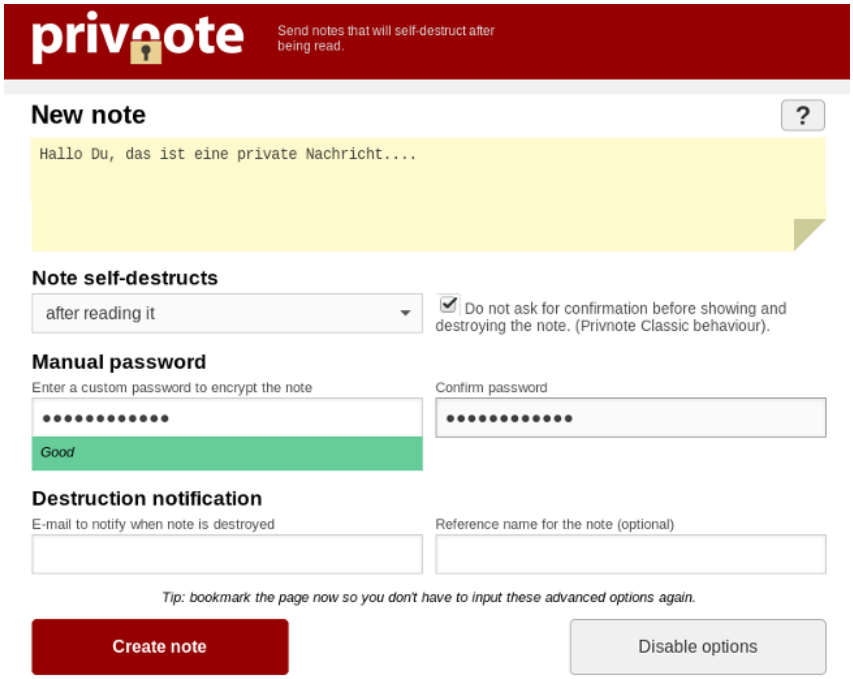


Abbildung 6.13: Eine Private Note schreiben

Den Link kann man per E-Mail dem Empfänger der Nachricht senden. Er kann die Nachricht im Browser abrufen. Nach dem Abruf der Nachricht wird sie auf dem Server gelöscht, sie ist also nur EINMALIG lesbar. Darauf sollte man den Empfänger hinweisen. Sollte die Nachricht nicht abgerufen werden, dann wird sie spätestens nach 30 Tagen gelöscht.

Man kann den Link NICHT über irgendwelche Kanäle in Social Networks (z.B. Facebook) versenden. Wenn man auf den Link klickt, läuft im Hintergrund ein Crawl der Seite bevor man weitergeleitet wird. Facebook holt sich die Nachricht und der Empfänger kommt zu spät.

PrivNote ist nicht kryptografisch abhörsicher wie die E-Mail Verschlüsselung mit OpenPGP. Wenn ein Angreifer unbedingt den Inhalt der Nachricht lesen will, kann er die Nachricht vor dem Empfänger abrufen und über den Inhalt Kenntnis erlangen. Der eigentliche Empfänger kann nur den Angriff erkennen, da die Nachricht auf dem Server gelöscht wurde. Damit sind die

Angebote für private Nachrichten geeignet, aber nicht geeignet für geheime oder streng vertrauliche Informationen.

6.4 ProtonMail, Tutanota und andere

Durch die Veröffentlichungen von Snowden/Greenwald sind viele hochmotivierte IT-Aktivisten angefeuert, neue Ideen und Konzepte für privacy-freundliche Dienste zu entwickeln. Die E-Mail Dienste ProtonMail.ch[30] (Schweiz), unseen.is[31] (Island) und Tutanota.de[32] möchte ich kurz vorstellen.

Diese E-Mail Dienste stellen einfache Benutzbarkeit von Verschlüsselung sowie Kompatibilität mit den gängigen E-Mail Protokollen in den Vordergrund und bemühen sich (im Rahmen ihrer Möglichkeiten) um bestmöglichen Schutz gegen staatlichen Zugriff.

Das Schreiben und Lesen von E-Mails erfolgt ausschließlich im Webinterface im Browser, ein E-Mail Client wie Thunderbird kann nicht verwendet werden. Das ermöglicht eine einfach nutzbare Verschlüsselung der Inhalte der E-Mails mit einer Krypto-Implementierung in Javascript im Browser, hat aber auch Nachteile.

Vorteile gegenüber Web.de, GMX.de, GMail.com u.a.

ProtonMail, unseen.is und Tutanota bieten viele Vorteile für Normalanwender, die Ihre E-Mails bisher im Webinterface von GMail, Yahoo! oder Hotmail bearbeiten.

- Die Provider respektieren die Privatsphäre der Nutzer, schnüffeln nicht in den Mails rum, geben keine Daten weiter und beobachten die Nutzer nicht beim Lesen von Newslettern.
- Die Provider bieten einen einfachen Zugang zur E-Mail Verschlüsselung für nicht-IT affine Nutzer. Man muss sich nur wenig mit der Verschlüsselung beschäftigen, um sie in der Praxis einsetzen zu können.
- Auch auf dem Smartphone ist verschlüsselte Kommunikation via E-Mail nutzbar. Tutanota und Protonmail bieten passende Apps im Google Playstore und für iPhones an.
- Die Daten werden verschlüsselt auf den Servern abgelegt. die Betreiber werben damit, dass sie keinen Zugriff auf den Klartext der Kommunikation haben. Die Kommunikation mit Partnern innerhalb des Dienstes ist automatisch Ende-zu-Ende verschlüsselt.
- Die SSL/TLS-Verschlüsselung für die Webseiten wird vom Qualsys SSL Server Test mit A+ bewertet. Tutanota unterstützt auch DANE/TLSA zur Verbesserung der Sicherheit der Transportverschlüsselung.

[30] https://protonmail.ch
[31] https://unseen.is
[32] https://tutanota.de

Am besten kommen die Vorteile zur Geltung, wenn alle Kommunikationspartner einen Account bei ProtonMail, unseen.is bzw. Tutanota haben.

Nachteile gegenüber Thunderbird+OpenPGP

Konzeptionell bedingt haben ProtonMail, unseen.is und Tutanota einige Schwächen. Die Verschlüsselung bietet nur hinreichende Sicherheit und ist für hohe Sicherheitsansprüche nicht geeignet.

- Die Nutzung von E-Mail Clients (wie von uns empfohlen) ist nicht vorgesehen, da die nötigen Protokolle nicht unterstützt werden. Damit entfällt auch die alternative Nutzung starker Kryptografie wie OpenPGP oder S/MIME. Das ist bei einigen genannten Diensten nicht möglich. Javascript ist für die Implementierung starker Kryptografie nur bedingt geeignet. Javascript wurde nicht als Programmiersprache für Krypto-Anwendungen entworfen. Best Practices für die Implementierung von Krypto sind mit Javascript nicht umsetzbar.
  - Javascript bietet keine Möglichkeiten, bei der Programmierung identische Ausführungszeiten für Code Verzweigungen zu erzwingen. Durch Seitenkanalangriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das ein Securitybug (z.B. CVE-2016-7056 ECDSA P-256 timing attack key recovery, OpenSSL).

    Seitenkanalangriffe auf Browser sind einfach, da der Rechner nicht kompromittiert werden muss. Das Script für den Angriff kann von einer beliebigen Webseite geladen werden, wie Forscher in *The Spy in the Sandbox – Practical Cache Attacks in Javascript* gezeigt haben.
  - Mit Javascript ist es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (*Overwriting memory - why?*[33]). Das normale Verhalten von Mailvelope wurde bei Tor Onion Router als Security Bug eingestuft.[34]
- Webanwendungen bieten viel mehr Angriffsmöglichkeiten als E-Mail Clients mit lokalen Tools zur Verschlüsselung. Thomas Roth demonstriert in dem Video *Hacking protonmail - with a browser*[35], wie man die Verschlüsselung von ProtonMail mit einem Browser und einfachen XSS-Hacks angreifen konnte. Die Lücken sind inzwischen beseitigt, vergleichbare Probleme hätte es bei Thunderbird aber nie geben können.
- Die Schlüssel werden im HTML5 Storage des Browsers gespeichert und sind somit leichter angreifbar. Im HTML5 Security Cheat Sheet[36]) wird vom OWASP empfohlen, keine sensitiven Informationen im HTML5 Storage des Browsers zu speichern, da diese Daten z.B. mit XSS-Angriffen kompromittiert werden könnten.

[33] http://www.viva64.com/en/k/0041
[34] http://heise.de/-1746523
[35] hhttp://vimeo.com/99599725
[36] hhttps://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

- Der Code für die Verschlüsselung wird durch die Webanwendung beim Aufruf der Webseite geladen oder aktualisiert. Außerdem werden die Schlüssel der Empfänger bei Bedarf vom Server geladen. Dieses Konzept nennt man *Server-basierte Kryptografie*. (Es ist damit nicht *Server-basierte Verschlüsselung* gemeint!) Das Konzept ist nicht neu. Es wurde bereits von Hushmail und Countermail eingesetzt (mit Java statt Javascript) oder Cryptocat (für Chats) und die Kritiken an diesem Konzept lassen sich auch für die oben genannten Dienste übernehmen.

  - Die Server-basierte Kryptografie von Hushmail wurde bereits 2007 von der US Drogenbehörde DEA kompromittiert[37]. Hushmail wurde gezwungen, die E-Mails von mehreren Accounts entschlüsselt bereitzustellen und musste der Aufforderungen nachkommen. Auch alle oben genannten Dienste könnten die Verschlüsselung unbemerkt kompromittieren, wenn sie es für staatliche Behörden tun müssten.
  - Server-basierte Kryptografie ist für hohe Sicherheitsansprüche politischer Aktivisten o.ä. generell nicht geeignet wie Patrick Ball in einem Essay bei Wired.com[38] ausführlich dargelegt.

  Tutanota und ProtonMail bieten inzwischen Apps für Android und iPhone an, die den Code für die Verschlüsselung enthalten und aus den Appstores installiert werden können. Auf dem Desktop PC kann man die Software von Tutatnota von Github auschecken und lokal installieren. Auch das schützt gegen Angriffe, ist allerdings deutlich komplizierter, als OpenPGP zur E-Mail Verschlüsselung zu nutzen.

[37] http://www.wired.com/2007/11/encrypted-e-mai
[38] http://www.wired.com/2012/08/wired_opinion_patrick_ball/all/

Kapitel 7

E-Mails verschlüsseln

Weltweit wird der unverschlüsselte E-Mail Verkehr systematisch gescannt. Führend ist die NSA mit *Echelon*, das auch zur Industriespionage sowie zum Abhören von NGOs verwendet wird, und Abhörschnittstellen bei allen großen amerikanischen ISPs. Frankreich betreibt ein ähnliches System unter dem Namen *French ECHELON*. Das russische Pendant zur NSA ist der SSSI (früher FAPSI). Der schwedische Geheimdienst FRA und das Schweizer Onyx Projekt nutzen Supercomputer zur Verarbeitung der abgeschnorchelten Datenmengen. Für Saudi Arabien, Syrien, Iran, Tunesien und Ägypten wurden entsprechende Aktivitäten nachgewiesen und die *Great Firewall* von China verfügt ebenfalls über die nötigen Features.

In Deutschland wird der E-Mail Verkehr im Rahmen der *Strategischen Fernmeldeaufklärung* von den Geheimdiensten gescannt. Eine von der G-10 Kommision genehmigte Stichwortliste mit 16.400 Begriffen (Stand 2010) wird für die automatisierte Vorauswahl verwendet, um nach Waffenhandel, Prolieferation und Terroristen zu suchen. Im Jahr 2010 meldeten die Scanner 37 Mio. E-Mails als verdächtig. 2011 hat der BND es geschafft, die automatisierten Scanner mit einem Spamfilter zu kombinieren, so dass "nur noch" 2,1 Mio. E-Mails als verdächtig gemeldet und kopiert wurden.

PGP, GnuPG und S/MIME sowie das neue PEP

PGP (*Pretty Good Privacy*) und die kostenlose Alternative GnuPG (*GNU Privacy Guard*) sowie S/MIME (*Secure MIME Protokoll*) sind fast 20 Jahre alte Standards für E-Mail Kryptografie. Sie können folgende Aufgaben erfüllen:

1. Mit dem **Verschlüsseln** von E-Mails wird die Vertraulichkeit des Inhalts der E-Mail gewährleistet. Eine Nachricht kann nur vom Empfänger mit dem paasenden Schlüssel geöffnet und gelesen werden.

2. Mit dem **Signieren** von E-Mails wird die Authentizität der Nachricht gewährleistet. Anhand der Signatur kann der Empfänger prüfen, ob eine Mail wirklich von dem angegebenen Absender kommt und unterwegs nicht modifiziert wurde.

3. Die Metadaten im Header der E-Mail (Absender, Empfänger, verwendete Software, evtl. die IP-Adresse des Absenders usw.) werden durch diese

beiden Verfahren nicht(!) verschleiert und können für die Kommunikationsanalyse verwendet werden.

PGP, GnuPG und S/MIME haben es in den letzten 20 Jahren nicht geschafft, eine massentaugliche Usability zu entwickeln. Wenn man erst einmal 20 Seiten Anleitung lesen muss, um die E-Mail Verschlüsselung zu verstehen, Software selbst konfigurieren muss, sich selbst die notwendigen Schlüssel erstellen muss oder beglaubigen lassen muss, sich um die Verteilung der Schlüssel selbst kümmern muss und es danach noch jedem Partner einzeln erklären muss, dann ist diese Krypto einfach nicht massentauglich.

PEP (*Pretty Easy Privacy*) ist relativ neu. Bisher gibt es nur wenig Software, die diese Variante der E-Mail Verschlüsselung unterstützt, für Thunderbird gibt es noch keine Lösung. PEP hat das Ziel, die Usability zu verbessern und damit eine breitere Anwendung von E-Mail Verschlüsselung zu ermöglichen. Man muss nur 5 Seiten Handbuch lesen, um die Verschlüsselung zu verstehen und der Schlüsseltausch wird deutlich vereinfacht.

Trotz der Hürden beim Einsatz lohnt es sich, dass man sich mit dem Thema E-Mail Verschlüsselung beschäftigt. E-Mail ist ein wichtiges Kommunikationsmedium, trotz des Booms der Messaging Dienste auf Smartphones.

Asymmetrische Verschlüsselung

PGP, GnuPG, S/MIME und PEP nutzen Asymmetrische Kryptografie. Das heißt, es werden unterschiedliche Schlüssel zum Verschlüsseln und zum Entschlüsseln verwendet:. Das Grundprinzip ist einfach erklärt:

- Jeder Anwender generiert ein Schlüsselpaar bestehend aus einem geheimen und einem öffentlichen Schlüssel. Während der geheime Schlüssel sorgfältig geschützt nur dem Anwender zur Verfügung stehen sollte, ist der öffentliche Schlüssel an alle Kommunikationpartner zu verteilen.
- Wenn Beatrice eine verschlüsselte Nachricht an Anton senden will, nutzt sie den öffentlichen Schlüssel von Anton, um die Nachricht zu chiffrieren. Nur Anton kann den Inhalt der E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.
- Wenn der Anton eine signierte E-Mail an die Beatrice senden will, erstellt er eine Signatur (digitale Unterschrift) mit seinem geheimen Schlüssel. Beatrice kann mit dem öffentlichen Schlüssel von Anton die Unterschrift und damit die Echtheit der Nachricht verifizieren, da nur Anton Zugriff auf seinen geheimen Schlüssel haben sollte.

Verschlüsselung und Signatur können kombiniert werden. Dabei wird der Inhalt der Nachricht zuerst signiert und dann alles zusammen (Nachricht + Signatur) verschlüsselt.

7.1 GnuPG und Thunderbird

Die folgende Anleitung erläutert den Einsatz von **GnuPG** in Kombination mit **Thunderbird**, dem E-Mail Client der Mozilla Foundation. Alle Komponenten stehen für Linux, Mac OS und WINDOWS kostenfrei zur Verfügung:

7.1.1 Installation von GnuPG

GnuPG ist eine frei nutzbare Implementierung des OpenPGP Standards zur Verschlüsselung und Signierung von Daten. Es wird vom GNU Projekt ständig weiterentwickelt. Das Thunderbird Add-on Enigmail verwendet standardmäßig GnuPG 2.x.

Windows: Das Projekt gpg4win [1] stellt ein Paket für Windows bereit mit GnuPG, dem GNU Privacy Assisten für die Schlüsselverwaltung und einer Erweiterung für den Windows Explorer.

MacOS: nutzen Sie die GPGTools [2].

Linux, BSD: installieren GnuPG 2.x nicht immer standardmäßig. In der Regel muss man es nachträglich installieren. Für Debian/Ubuntu funtioniert:

```
> sudo apt install gnupg2 gpg-agent pinentry-gtk2 scdaemon
```

Bei einigen Linux Dsitibutionen ist *gpg-agent* im Paket *gpgsm* enthalten. Der *gpg-agent* wird für die Eingabe der Passphrase benötigt und sollte beim Login automatisch gestartet werden. Dafür fügt man in der Konfiguration *$HOME/.gnupg/gpg.conf* folgende Zeile am Ende ein:

```
use-agent
```

In der Datei *$HOME/.gnupg/gpg-agent.conf* kann man konfigurieren, wie lange der Agent die Passphrase für einen Key speichert. Standardmäßig wird eine Passphrase 10min (600s) gespeichert. GPA ändert den Wert aus Sicherheitsgründen auf 300s.

```
default-cache-ttl 300
max-cache-ttl 360
```

7.1.2 Verbesserte Konfiguration von GnuPG

In der Konfigurationsdatei *gpg.conf* kann man nach der Installation ein paar kleine Verbesserungen vornehmen. Die Konfigurationsdatei findet man unter Windows in *%APPDATA%/GnuPG* und unter Linux/BSD im Verzeichnis *$HOME/.gnupg*.

Die Datei kann man mit einem Texteditor bearbeiten und folgende Optionen ergänzen bzw. durch Entfernen des Kommentarzeichens # aktivieren:

[1] http://www.gpg4win.org
[2] http://www.gpgtools.org

```
# keine Informationen über ersion und Betriebssystem einfügen
no-emit-version
no-comments

display-charset utf-8

# 16-stellige Key-IDs verwenden statt 8-stelliger (schwerer zu faken)
keyid-format 0xlong

# Keyserver-URLs in Keys ignorieren (Tracking möglich)
keyserver-options no-honor-keyserver-url, no-auto-key-retrieve, no-include-revoked

# Empfohlene Preferenzen für Schlüsselgenerierung vom
# Debian-Team: http://keyring.debian.org/creating-key.html
personal-digest-preferences SHA512
cert-digest-algo SHA512
default-preference-list SHA512 SHA384 SHA256 SHA224 AES256 AES192
                        AES CAST5 ZLIB BZIP2 ZIP Uncompressed

# sonstiges
fixed-list-mode
verify-options show-uid-validity
list-options show-uid-validity
```

7.1.3 Installation der Enigmail-Erweiterung

Enigmail [3] ist eine Erweiterung für Mozilla Thunderbird, welche eine Schnittstelle zu GnuPG bereitstellt und den Umgang mit Verschlüsselung im täglichen E-Mail Chaos vereinfacht. Am einfachsten installiert man Enigmail mit dem Add-on Manager von Thunderbird. Den Manager findet man unter *Extras - Add-ons*. Im Suchfeld gibt man *Enigmail* ein. Ein Klick auf den Button *Installieren* holt das Add-on.

Unter Linux kann man Enigmail auch mit dem bevorzugten Paketmanager installieren. Für Debian und Ubuntu kann man *aptitude* nutzen:

```
> sudo apt install enigmail
```

Unter NetBSD und OpenBSD muss man Thunderbird mit Enigmail neu kompilieren. In der Datei *mk.conf* ist dafür folgende Option zu setzen:

```
PKG_OPTIONS.thunderbird=mozilla-enigmail
```

Nach Installation von Enigmail muss Thunderbird neu gestartet werden! Nach dem Neustart kann man den Konfigurations-Assistenten unter *OpenPGP - OpenPGP-Assistent* aufrufen. Dabei werden folgende Schritte durchlaufen:

1. Abfrage, ob gesendete E-Mails standardmäßig signiert und verschlüsselt werden sollen. Um unbedarfte Anwender nicht zu verwirren, kann man diese Funktion deaktivieren.

[3] http://enigmail.mozdev.org

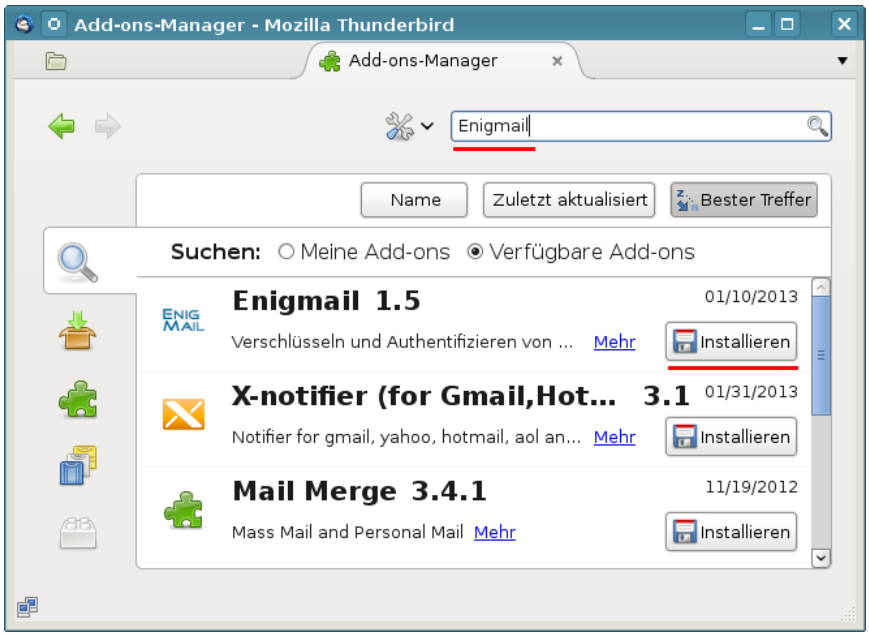


Abbildung 7.1: Installation von EnigMail

2. Abfrage, ob gesendete E-Mails standardmäßig verschlüsselt werden sollen. Da man meist nur OpenPGP-Schlüssel von wenigen Empfängern hat, kann man diese Option zunächst deaktivieren. Später, wenn sich die Verschlüsselung im Bekanntenkreis durchgesetzt hat, ist eine Aktivierung vielleicht sinnvoll.

3. Optimierung der Einstellungen für GnuPG. Die Vorgaben sind sinnvoll und sollten übernommen werden.

4. Generieren der Schlüsselpaare für alle vorhandenen Konten. Die Passphrase für den Zugriff auf den privaten Key sollte man sich vorher gut überlegen und merken! Es heißt *Passphrase* und nicht *Passwort*. Die Passphrase darf ruhig etwas länger sein und auch Leer- bzw. Sonderzeichen enthalten.

   Die Vorschläge des Assitenten sind erst einmal sinnvoll. Individuelle Anpassungen (z.B. 4096 Bit Schlüssellänge usw.) kann man nur beim Erstellen eines neuen Schlüssels in der Schlüsselverwaltung wählen.

   Kryptografischen Funktionen können nicht unbegrenzt den Fortschritten der Kryptoanalys widerstehen. Es ist sinnvoll, die Nutzungszeit des Schlüssels mit einem Haltbarkeitsdatum zu versehen. Eine Nutzung länger als **5 Jahre** sollte man nur in begründeten Ausnahmen in Erwägung ziehen. Bei der Schlüsselerstellung sollte ein Verfallsdatum angegeben werden.

Mit jedem Schlüsselpaar kann auch ein Zertifikat für den Rückruf erstellt und sicher gespeichert werden. Mit diesem Zertifikat kann man einen Schlüssel für ungültig erklären, wenn der private Key kompromittiert wurde oder die Passphrase in Vergessenheit gerät.
Dieser 4. Schritt kann übersprungen werden, wenn man bereits gültige OpenPGP Schlüssel hat.

5. FERTIG

7.1.4 Schlüsselverwaltung

Die Schlüsselverwaltung findet man in Thunderbird unter dem Menüpunkt *Enigmail - Schüssel verwalten*. Ist die Liste noch leer, wählt man zuerst den Menüpunkt *Erzeugen - Neues Schlüsselpaar*. Diesen Schritt übernimmt jedoch auch der Assistent zur Einrichtung von Enigmail.

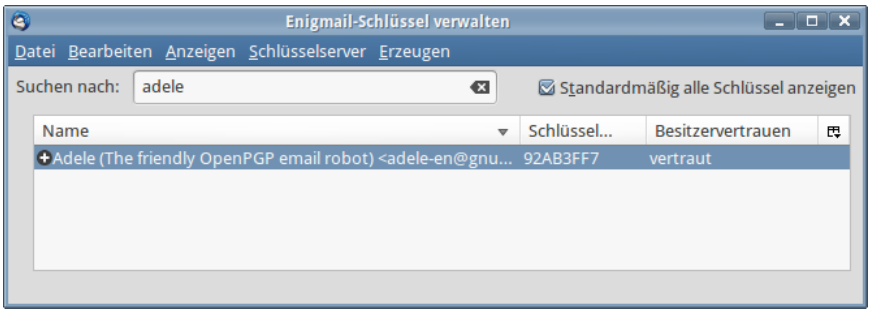
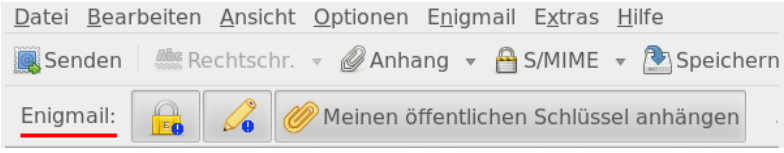


Abbildung 7.2: Schlüsselverwaltung von EnigMail

Exportieren des eigenen öffentlichen Schlüssels

Um verschlüsselt zu kommunizieren, muss den Kommunikationspartnern der eigene öffentliche Schlüssel zur Verfügung gestellt werden. Dafür gibt es mehrere Möglichkeiten:

- Man kann den eigenen öffentlichen Schlüssel als E-Mail Anhang versenden. Um den Schlüssel als Attachment an eine Mail anzuhängen, aktiviert man die Option *Meinen öffentlichen Schlüssel anhängen* beim Schreiben einer E-Mail in der Enigmail Toolbar.



- Man kann den eigenen öfffentlichen Schlüssel auf einem Webserver ablegen. Den Menüpunkt für den Export in eine Datei findet man unter *Datei -> Schlüssel exportieren* in der Schlüsselverwaltung. Diese Textdatei kann

man z.B. im eigenen Blog zum Download anbieten. Viele E-Mail Provider bieten auch einen kleinen Cloud Speicher für Daten. Man kann die Datei mit dem öffentlichen Key hochladen und für alle zum Download freigeben. In der E-Mail Signatur könnte man auf den Download hinweisen.

- Man zur Verteilung auch die Schlüsselserver im Internet nutzen. In der Schlüsselverwaltung findet man den Menüpunkt *Schlüssel-Server -> Schlüssel hochladen*. Der öffentliche Schlüssel wird auf den Schlüsselserver exportiert und steht dort allen Partnern zur Verfügung. Die verschiedenen Server synchronisieren ihren Datenbestand.

  Hinweis: Beim Upload auf die Keyserver erfolgt keine Verifizierung der Identität! Jeder kann beliebige Schlüssel für beliebige E-Mail Adressen auf Keyservern veröffentlichen.

Import der Schlüssel der Partner

Um an einen Kommunikationspartner verschlüsselte E-Mails zu senden oder die Signatur erhaltener Nachrichten zu prüfen, benötigt man den öffentlichen Schlüssel des Partners.

- Am einfachsten läßt sich dieser importieren, wenn man eine signierte E-Mail erhalten hat. Ein Klick auf den blauen Stift rechts oben im Header der E-Mail reicht aus, um den öffentlichen Schlüssel von einem Schlüsselserver zu importieren.
- Zum Importieren des Schlüssel eines Partners aus einer Datei, die man als Attachement oder per Download erhalten hat, wählt man den Menüpunkt *Datei / Importieren* in der Schlüselverwaltung.
- Wenn der Schlüssel als Text angeboten wird, sieht es etwa so aus:


  ```
  -----BEGIN PGP PUBLIC KEY BLOCK-----
  Version: SKS 1.1.1

  mQENBEt5GIIBCACOnOeTtfBIUbdcOmw5DlLuxkQB4uQ/8HbSUaH96s1z
  HqFA/31GB7OpodyEKqc41T2TDdWWITfdy1dpxeGwopBK/wljPAuNAgJQ
  ....
  fU7xEW/RQT76nORfTXnbj2m/DRPmoivcXW5G/zJM6QUjl++vO7OB+3xb
  SnDCMQtaWHM57eLcmnsMAK3qHOYlVrNUTSvEgatjUqLU
  =fP9T
  -----END PGP PUBLIC KEY BLOCK-----
  ```


  Man kann die Zeilen von BEGIN ...bis... END mit der Maus markieren und in die Zwischenablage kopieren. In der Schlüsselverwaltung von Enigmail importiert man den Schlüssel wie im Bild 7.3 dargestellt mit *Bearbeiten - Aus Zwischenablage importieren*.

- Man kann die OpenPGP Keyserver nach einem passenden Schlüssel durchsuchen (siehe unten). Dabei sollte man nach Möglichkeit den Fingerprint des Schlüssels als Suchkriterium wählen und nicht die E-Mail Adresse des Empfängers, da jeder einen falschen Schlüssel für eine E-Mail Adresse hochladen kann.

Abbildung 7.3: OpenPGP-Schlüssel aus Zwischenablage importieren

7.1.5 Signieren und Verschlüsseln erstellter E-Mails

Wurde in den Kontoeinstellungen in der Sektion *OpenPGP* die Option *Nachrichten standardmäßig verschlüsseln* aktiviert, sind beim Schreiben einer E-Mail keine weiteren Hinweise zu beachten. Anderenfalls muss man für jede E-Mail explizit festzulegen, dass sie verschlüsselt werden soll.

Das Fenster für das Erstellen einer neuen E-Mail zeigt nach der Installation von Enigmail eine neue Toolbar mit Buttons zum Verschlüsseln, Signieren und Anhängen des eigenen public Keys (Bild 7.4).

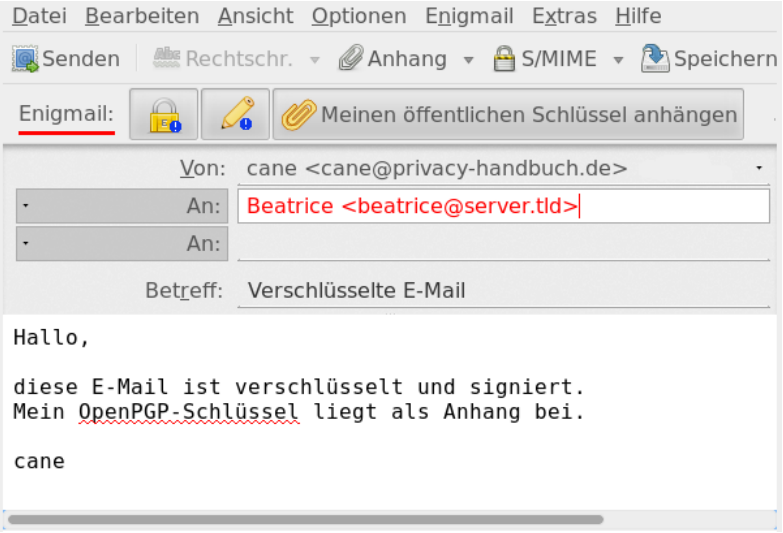


Abbildung 7.4: Signieren und Verschlüsseln einer E-Mail

Sollte die E-Mail Anhänge enthalten, ist die Option *PGP / MIME* zu aktivieren, um die Attachements standardkonform zu verschlüsselt.

Achtung: Die Betreffzeile wird nicht (!) mit verschlüsselt. Sicher wird man die Kontonummer nicht in der Betreffzeile schreiben, aber auch ein ausführlicher Betreff ermöglicht zusammen mit der/den Adressen der Empfänger einige Aussagen über die Kommunikation.

Wenn man als Betreff beispielsweise schreibt:

Treffen der Aktivisten-Gruppe ... am 13.01.09

und diese Mail per CC an alle Mitglieder der Gruppe versendet, sind 90% der relevanten Informationen bekannt und man kann sich die Verschlüsselung der Mail sparen.

Soll jede versendete E-Mail verschlüsselt werden, wenn der Schlüssel des Empfängers vorhanden ist, kann die entsprechende Option in den Einstellungen von Enigmail aktiviert werden (Bild 7.5). Alternativ ist es auch möglich, lediglich für bestimmte Empfänger festzulegen, dass alle E-Mails signiert oder verschlüsselt werden sollen. Diese Regeln kann man unter *Enigmail -> Empfängerregeln* definieren.

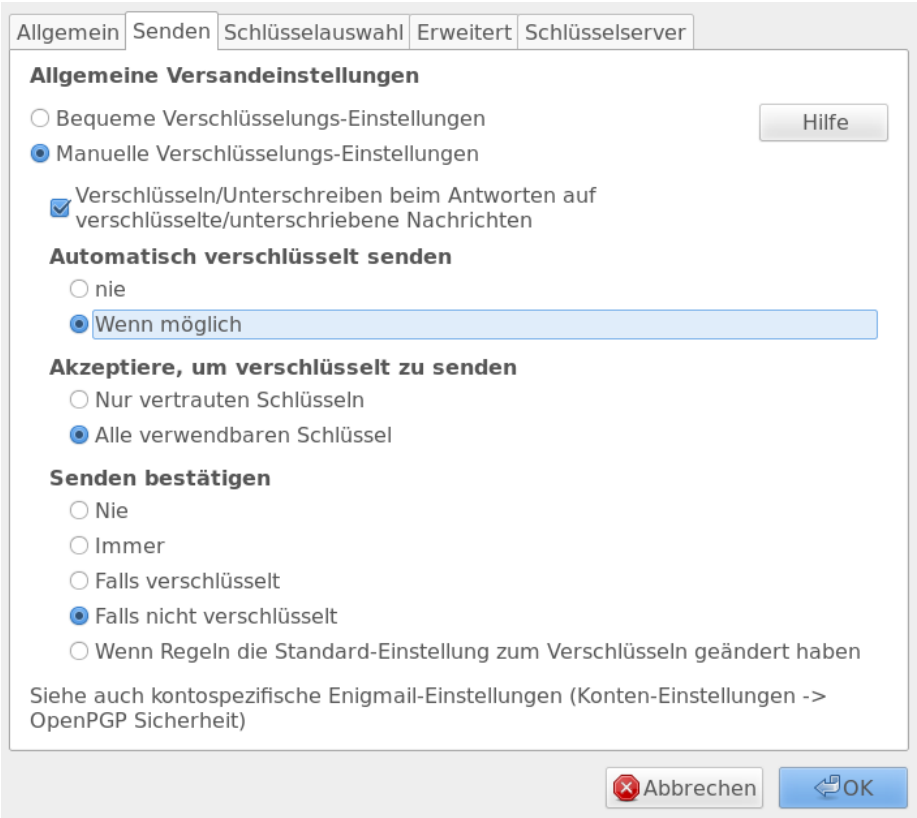


Abbildung 7.5: Signieren und Verschlüsseln aller E-Mails, wenn möglich

7.1.6 Adele - der freundliche OpenPGP E-Mail-Roboter

Adele ist der freundliche OpenPGP E-Mail-Roboter der G-N-U GmbH. Man kann mit dem Robot seine ersten verschlüsselten Mails austauschen und ein wenig üben ohne Freunde mit Anfängerprobleme zu belästigen.

1: Den eigenen Schlüssel an Adele senden: Als erstes schickt man den eigenen öffentlichen Schlüssel per E-Mail an *adele@gnupp.de*. Den Schlüssel

hängt man als Anhang an die Mail an, indem man die Option *OpenPGP - Meinen öffentlichen Schlüssel anhängen* vor dem Versenden der Mail aktiviert (Bild **??**)

2. **Verschlüsselte Antwort von Adele:** Als Antwort erhält man nach einigen Minuten eine verschlüsselte E-Mail von Adele. Die E-Mail wird nach Abfrage der Passphrase entschlüsselt und enthält den Schlüssel von Adele:

```
Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ihr öffentlicher Schlüssel wurde von mir empfangen.

Anbei der öffentliche Schlüssel von adele@gnupp.de,
dem freundlichen E-Mail-Roboter.

Viele Grüße,
adele@gnupp.de

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.9 (GNU/Linux)

mQGiBDyFlIkRBACfVHJxv47r6rux7TwT4jHM7z/2VfyCrmcRegQEsbdLfqu3mEmK
RouuaDQukNINWk2V2ErOWzFnJqdzpapeuPJiOWpOuIEvU3FRPhYlytw9dFfwAHv4
MJ7639tAx9PfXBmZOd1PAoE451+VLhIGlLQiFGFppJ57SZ1EQ71/+/nkSwCg8Mge
....
EQIABgUCPIWUlQASCRDlczRpkqs/9wdlR1BHAAEBv2OAoJJGeeZjMCSbXtmNSwfW
QsLOdO+4AKCdXwt552yi9dBfXPo8pB1KDnhtbQ==
=ERT8
-----END PGP PUBLIC KEY BLOCK-----
```

3. **Schlüssel von Adele importieren:** Man kann die Zeilen von `BEGIN PGP PUBLIC KEY BLOCK` bis einschließlich `END PGP PUBLIC KEY BLOCK` mit der Maus markieren, in die Zwischenablage kopieren und in der Schlüsselverwaltung über *Bearbeiten - Aus Zwischenablage importieren* einfügen.

   Alternativ holt man sich Adeles Schlüssel mit der ID 0x92AB3FF7 von einem Keyserver.

4. **Adele verschlüsselte E-Mails schreiben** Jetzt kann man Adele verschlüsselte E-Mails schicken. Als Antwort erhält man umgehend eine gleichfalls verschlüsselte E-Mail mit dem gesendeten Text als Zitat.

```
Hallo,

hier ist die verschlüsselte Antwort auf Ihre E-Mail.

Ich schicke Ihnen Ihre Botschaft im Wortlaut zurück, damit Sie
sehen, dass ich sie erfolgreich entschlüsseln konnte.
```

```
> Hello Adele,
>
> hope you are feeling well.
```

7.1.7 Verschlüsselung in Webformularen

Auch bei der Nutzung eines Webmail Accounts oder Webforms für die Versendung anonymer E-Mails muss man auf Verschlüsselung nicht verzichten.

Einige grafische Tools für die Schlüsselverwaltung wie z.B. GPA (*GNU Privacy Assistent*) [4] oder KGPG enthalten einen Editor. Man kann den Text in diesem Editor schreiben, mit einem Klick auf den entsprechenden Button signieren oder verschlüsseln und das Ergebnis über die Zwischenablage in die Textbox der Website einfügen. Entschlüsseln funktioniert umgekehrter.

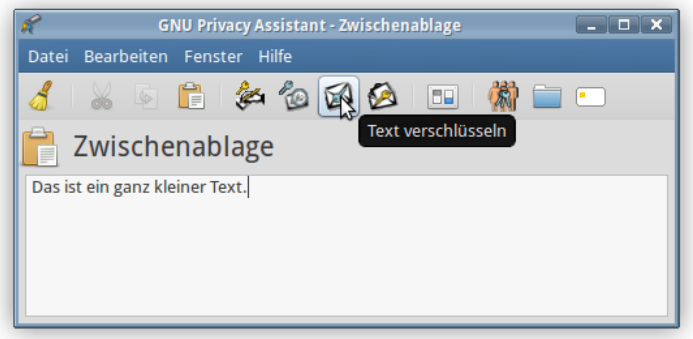


Abbildung 7.6: Text mit GPA verschlüsseln

Enthält das bevorzugte Tool für die Schlüsselverwaltung keinen Texteditor, kann man folgende Alternativen nutzen, die auch für unterwegs (auf dem USB-Stick) geeignet sind:

1. Das kleine Tool **gpg4usb** [5] bietet einen Editor mit den Buttons für das Ver- und Entschlüsseln des Textes, Dateiverschlüsselung sowie eine kleine Schlüsselverwaltung. Das ZIP-Archiv enthält Versionen für Windows und Linux. Es kann einfach auf dem USB-Stick genutzt werden.

2. **Portable PGP** [6] ist eine Java-Anwendung (plattformunabhängig), die ebenfalls Texte und Dateien ver- und entschlüsseln kann. Eine einfach Schlüsselverwaltung ist ebenfalls enthalten. Zusätzlich zu Portable PGP benötigt man eine Java Laufzeitumgebung. Eine portable Version der Sun-JRE gibt es bei portableapps.com.

[4] http://www.gnupg.org/related_software/gpa/index.de.html
[5] http://www.gpg4usb.org/
[6] http://ppgp.sourceforge.net

7.1.8 Browser Add-ons wie Mailevelop

Browser Add-ons wie *Mailevelop* oder *Web PG* empfehle ich aus folgenden Gründen nicht:

1. Die Schlüssel werden im HTML5 Storage des Browsers gespeichert und sind damit leichter angreifbar als bei der Verwaltung durch ein lokal installiertes GnuPG Tool.

2. Javascript ist für starke Kryptografie nur bedingt geeignet. Es gibt z.B. keine Möglichkeit, Speicherbereiche im PAM (Hauptspeicher) gezielt zu überschreiben. Entsperrte Keys bleiben nach der Verwendung im RAM erhalten, wo sie durch eine Schadsoftware ausgelesen werden könnten. Bei Tor war dieses Verhalten ein schwerer Bug, aber bei der Verschlüsselung von Mails wird dieses Verhalten einfach pauschal akzeptiert?

7.1.9 GnuPG Smartcard nutzen

Die Sicherheit asymmetrischer Verschlüsselung hängt von der sicheren Aufbewahrung des privaten Svhlüssels ab. Es gibt mehrere Möglichkeiten, wie privaten Keys kompromittiert werden könnten:

- Wenn man GnuPG auf mehreren Computern nutzt, auf denen andere Nutzer Administrator- bzw. Root-Privilegien haben, könnten die privaten Keys von Administratoren eingesammelt werden.

- Böswillige Buben können mit einem Trojaner versuchen, den privaten Key zu kopieren und die Passphrase mit Keyloggern oder mit Tools wie *Elcomsoft Distributed Password Recovery* ermitteln.

- Die unbedachte Entsorgung einer Festplatte oder eines Computers ist ein weiteres Risiko, wenn die privaten Daten nicht sicher gelöscht wurden.

Smartcards ermöglichen eine sichere Nutzung von GnuPG unter diesen Bedingungen. Der private Key ist nicht auf dem Rechner sondern ausschließlich auf der Smartcard gespeichert, er verläßt diese sichere Umgebung nicht und alle Krypto-Opertionen, die den privaten Schlüssel nutzen, werden auf der Smartcard ausgeführt. Die Nutzung von Smartcards hätte wahrscheinlich die Kompromittierung der OpenPGP-Schlüssel von Cryptome.org[7] verhindern können.

Ein paar Angebote für OpenPGP Smartcards:

- Die **GnuPG-Smartcard** gibt es im shop.kernelconcepts.de[8]. Die Bestellung erfolgt per E-Mail und man braucht zusätzlich einen Smartcard Reader oder den ebenfalls dort erhältlichen Gemalto USB Adapter.

[7] http://heise.de/-2817797
[8] http://shop.kernelconcepts.de

- Der **NitroKey**[9] ist ein Open Source Hardware Projekt und der Nachfolger des Cryptostick. Der NitroKey Pro enthält zusätzliche einen OTP-Generator und Passwortspeicher. (Für die Nutzung dieser Zusatzfunktion ist die NitroKey App[10] zu installieren.)

- Der **Yubikey 4** ist ein One-Time-Passwordgenerator (OTP), den man für sichere Logins bei verschiedenen Wsebdiensten nutzen kann. Er enthält zusätzlich eine OpenPGP Smartcard.[11]

Erster Test

Die GnuPG Software Collection kann Smartcards *out-of-the-box* nutzen. Zuerst sollte man prüfen, ob alles funktioniert und die Smartcard erkannt wird. Smartcard anschließen und auf der Konsole bzw. in der DOS-Box folgendes Kommando eingeben:

```
> gpg2 --card-status
Application ID ...: D27600xxxxxxxxxxxxxxx
Version ..........: 2.0
Manufacturer .....: unknown
...
```

Wenn keine Smartcard gefunden wird, kann man zuerst prüfen, ob die GnuPG Software Collection vollständig installiert wurde (*gpg2 + gpg-agent + scdaemon*) und ob der gpg-agent läuft. Bekannte Probleme gibt es auch mit dem GNOME Keyring Manager (siehe unten).

Smartcards mit Enigmail oder GPA nutzen

Enigmail und der GNU Privacy Assistent sind voll kompatibel mit Smartcards und bieten eine grafische Oberfläche, um Smartcards zu verwalten. Diese Funktionen öffnet man über den Menüpunkt *Enigmail - Smartcard verwalten*.

1. Als Erstes kann man die Card personalisieren, den Namen usw. editieren, eine Download URL für den Public Key angeben... (*Edit Card Data*).

2. Im zweiten Schritt sollte der PIN und der Admin-PIN geändert werden. Der PIN ist ein Passwort, mit dem der Nutzer den Zugriff auf den privaten Key auf der Smartcard freigibt (Default: 123456). Der Admin-PIN ist ein Passwort zum Ändern der Daten und der Schlüssel auf der Smartcard. (Default: 12345678).

   Die eigenen PINs können maximal 32 Zeichen lang sein und neben Zahlen auch Buchstaben enthalten. *Passwort* wäre eigentlich eine bessere Bezeichnung. Wurde der PIN 3x falsch eingegeben, wird die Card gesperrt und kann mit dem Admin-PIN wieder entsperrt werden (*Unblock*

[9] https://www.nitrokey.com/de
[10] https://www.nitrokey.com/de/download
[11] https://www.yubico.com/products/yubikey-hardware/

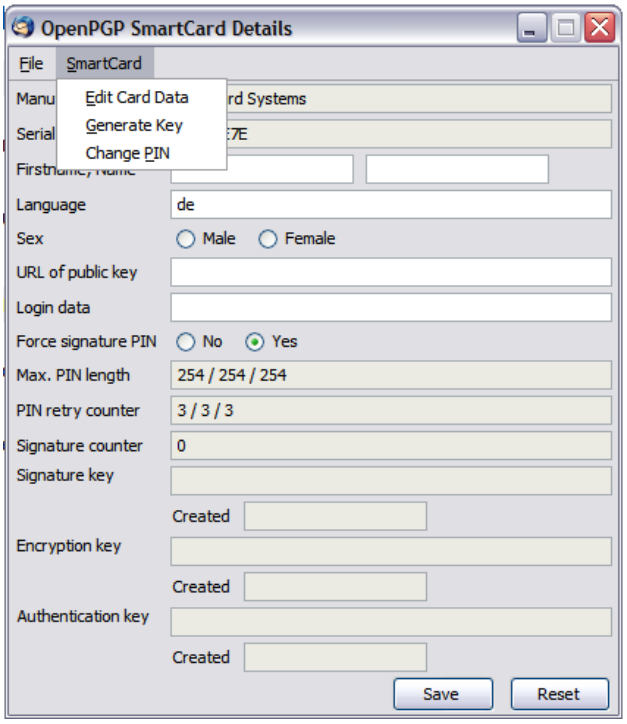


Abbildung 7.7: Smartcard verwalten

PIN). Wird der Admin-PIN 3x falsch eingegeben, ist die Smartcard zerstört!.

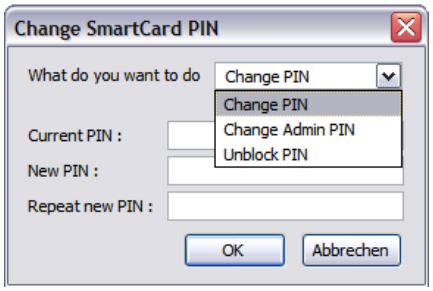


Abbildung 7.8: Smartcard-PINs ändern

3. Als letzten Schritt vor der Nutzung der Smartcard im täglichen Krypto-Chaos sind die Keys auf der Smartcard zu generieren. Der entsprechende Dialog bietet die Auswahl eines Mail-Account an, für den die Smartcard genutzt werden soll. Für diesen Account darf kein(!) OpenPGP-Key vorhanden sein. Anderenfalls bricht der Vorgang mit einer wenig verständlichen Fehlermeldung ab.

Man kann bei der Erzeugung des Schlüssels ein Passwort-gesichertes Backup der Card-Keys anlegen. Später ist kein Zugriff auf diese Schlüssel mehr möglich. Bei Beschädigung der Smartcard kann der gesicherte Card-Key in eine neue Smartcard importiert werden. Das Backup wird im GnuPG-Verzeichnis abgelegt und ist auf einem sicheren Datenträger zu speichern!

Wurden die Schlüssel erfolgreich generiert, findet man in der *Schlüsselverwaltung* ein neues Paar. Der Public Key dieses Schlüsselpaares kann wie üblich exportiert und den Partnern zur Verfügung gestellt werden. Der Private Key dieses Paares definiert lediglich, dass die kryptografischen Operationen auf einer Smartcard auszuführen sind. Er ist ohne die passende Card unbrauchbar.

Funktionen für Genießer

Die Nutzung von gpg2 auf der Kommandozeile bietet etwas mehr Möglichkeiten, als die GUIs von Enigmail oder GPA zur Verfügung. Natürlich stehen auch die mit dem GUI durchführbaren Funktionen auf der Kommandozeile zur Verfügung. Einen Überblick über alle Smartcard-Funktionen gibt die Hilfe mit dem *help* Kommando. Als erstes muss man den Admin Mode aktivieren, dann hat man vollen Zugriff auf alle Funktionen:

```
> gpg2 --card-edit
...
gpg/card> admin
Admin-Befehle sind erlaubt

gpg/card> help
...
gpg/card> quit
```

Neue Schlüssel generiert man auf der Smartcard mit *generate*, die PIN und Admin-PIN kann man mit *passwd* ändern, mit *unblock* kann man den Zähler für Fehlversuche zurück setzen und *factory-reset* löscht alle Schlüssel auf der Smartcard.

Neuer oder fremder Rechner - was nun?

Ein nettes Feature von OpenPGP Smartcards ist es, an einem neuen oder fremden Rechner den Public Key von einer Download Adresse holen zu können. Der private Key ist auf der Card in einer sicheren Umgebung, somit kann man auch unterwegs auf einem halbwegs vertrauenswürdigen, fremden Rechner eines Bekannten mit vollständiger GnuPG Installation die PGP-Verschlüsselung nutzen ohne den privaten Schlüssel zu kompromittieren.

Die Funktion zum Download des Public Key steht nur auf der Kommandozeile zur Verfügung. Nach dem Abrufen des Public Key von der Downoad URL muss man noch einmal den Card-Status aufrufen, damit der private Schlüssel an den Public Key gebunden wird:

```
> gpg2 --card-edit
...
gpg/card> fetch        (Abrufen des Public Key von der Download URL)
gpg/card> quit
...
> gpg2 --card-status    (Re-bind von private und public Key)
...
```

Vorhandenen Schlüssel weiter verwenden

Wenn man bereits PGP für die Verschlüsselung nutzt und einen vorhandenen Schlüssel weiter verwenden möchte, dann kann man die Private Keys dieses Schlüssel auch auf eine OpenPGP Smartcard übertragen. Damit erspart man sich die Verteilung eines neuen Schlüssels und kann die Beglaubigungen des Web-of-Trust behalten.

GnuPG erstellt standardmäßig Schlüsselpaare mit einem Hauptschlüssel zum Signieren und Beglaubigen sowie einen Unterschlüssel zum Verschlüsseln. Die OpenPGP Smartcard kennt drei Schlüssel, einen Schlüssel zum Signieren, einen Schlüssel zum Verschlüsseln und einen Schlüssel zum Authentifizieren. Man muss den von GnuPG erstellten Haupt- und Unterschlüssel einzeln auf die korrespondierenden PLätze auf der Smartcard schieben.

Als erstes ruft man *gnupg2* mit der *edit-key* Funktion für den Schlüssel auf, den man auf die Smartcard verschieben will. Mit *toggle* schaltet man auf die Verwaltung der privaten Keys. Dann schiebt man mit *keytocard* zuerst den Hauptschlüssel als Signatur Key auf die Smartcard, wählt den Subkey mit *key 1* aus und schiebt den Encryption Subkey auf den passenden Platz auf der Smartcard.

```
> gpg2 --edit-key mustermann@server.tld
Geheimer Schlüssel ist vorhanden.
...
gpg> toggle

sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb  rsa2048/08D68793
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E


gpg> keytocard
Den Hauptschlüssel wirklich verschieben? (j/N) j
Wählen Sie den Speicherort für den Schlüssel:
    (1) Signatur-Schlüssel
    (3) Authentisierungs-Schlüssel
Ihre Auswahl? 1

gpg> key 1
```

```
sec  rsa2048/8A02F3F6
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: SC
ssb*  rsa2048/08D68793
     erzeugt: 2016-06-18  verfällt: niemals   Aufruf: E

gpg> keytocard
Wählen Sie den Speicherort für den Schlüssel:
   (2) Verschlüsselungs-Schlüssel
Ihre Auswahl? 2

gpg> quit
Änderungen speichern? (j/N) j
```

Danach kann man den Status der Smartcard prüfen und sich davon überzeugen, dass die beiden Schlüssel jetzt als *Signature key* und *Encryption key* auf der Smartcard liegen:

```
> gpg2 --card-status

Reader ...........: 20A0:4108:000036C40000000000000000:0
Application ID ...: D2760001240102010005000036C40000
Version ..........: 2.1
...
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: C5DF 0BB0 11B7 3F49 3A37  AFC4 4472 A2E8 8A02 F3F6
      created ....: 2016-06-18 15:32:07
Encryption key....: 94E1 D64A 51C0 8C78 CE60  6472 0059 00DC 08D6 8793
      created ....: 2016-06-18 15:32:07
Authentication key: [none]
General key info..: pub  rsa2048/8A02F3F6 <mustermann@server.tld>
sec   rsa2048/8A02F3F6  erzeugt: 2016-06-18  verfällt: niemals
ssb   rsa2048/08D68793  erzeugt: 2016-06-18  verfällt: niemals
```

7.1.10 OpenPGP Keyserver

Die OpenPGP Keyserver bilden eine Infrastruktur im Web, um öffentliche Schlüssel auch Unbekannten zum Download anzubieten. Die verschiedenen Server synchronisieren ihren Datenbestand. Man kann die Keyserver nach einem passenden Schlüssel durchsuchen.

- Auf der Kommandozeile bzw. DOS-Box kann man nach OpenPGP Schlüsseln anhand der E-Mail Adresse suchen und einen der gefundenen Schlüssel importieren:

  ```
  > gpg2 --search cane@privacy-handbuch.de
  ```

  Wenn man die Key-ID oder den Fingerprint des Schlüssels kennt und weiss, dass der Schlüssel auf einem Keyserver zu finden ist, kann man ihn auch direkt importieren:

```
> gpg2 --recv 0x8F1E7F49912F0D9B73586C908CD51D2D7E36E399
```

- In Enigmail findet man die Suchfunktion in der Schlüsselverwaltung unter dem Menüpunkt *Schlüssel-Server -> Schlüssel suchen*.

Vorsicht bei der Nutzung von Keyservern

Man kann auf den Keyservern nach Schlüsseln anhand E-Mail Adressen (1), 8-stellige oder 16-stellige Key IDs oder dem bekannten Fingerprint (4) suchen.

1. Wenn man nach der E-Mail Adresse sucht, dann werden unter Umständen mehrere Schlüssel zum Importieren angeboten. Es gibt immer wieder Witzbolde, die Schlüssel für fremde E-Mail Adressen auf den Keyservern hochladen (um die Verschlüsselung zu stören?).

   Wenn man zum Beispiel den Schlüssel von Felix v. Leitner (Fefe) sucht, dann findet man fünf Schlüssel. Aber nur der Schlüssel von Okt. 2013 ist korrekt (nicht der neueste Schlüssel!), wie Fefe in seinem Blog schreibt.[12]

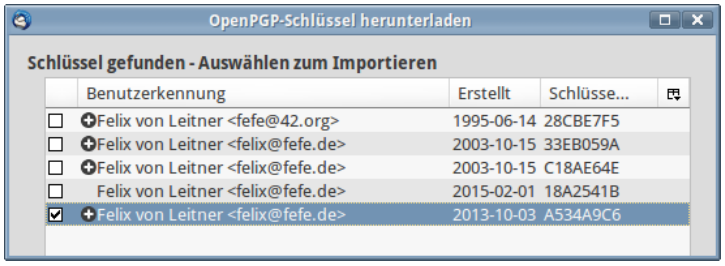


Abbildung 7.9: Fünf OpenPGP-Schlüssel für eine E-Mail Adresse

   J. Schmidt von Heise.de beklagt, dass ein Scherzkeks OpenPGP Schlüssel für seine E-Mail Adresse auf die Keyserver hochgeladen hat und dass er damit verschlüsselten E-Mails nicht lesen kann (Editorial c't 6/2015).

   Erinn Clark signierte die Downloads des TorBrowserBundle. Für ihre E-Mail Adresse wurden Fake Schlüssel auf den Keyserver publiziert.[13]

   Gavin Andresen signierte die Bitcoin Binaries, für seine E-Mail Adresse wurden ebenfalls Fake Schlüssel auf den Keyserver publiziert.[14]

2. Statt E-Mail Adressen kann man auch nach der 8-stelligen Key-ID suchen (zB. 0xA534A9C6). Diese Methode liefert besser Ergebnisse, allerdings muss man die richtige Key-ID kennen. Auch diese Methode ist nicht sicher, da man diese Key-IDs ebenfalls faken kann, wie ein Forscherteam demonstrierte.[15]

[12] https://blog.fefe.de/?ts=aa27d652
[13] https://lists.torproject.org/pipermail/tor-talk/2014-March/032308.html
[14] http://gavintech.blogspot.ch/2014/03/it-aint-me-ive-got-pgp-imposter.html
[15] http://heise.de/-2473281

3. Die 16-stellige Key-ID (zB. 0xFC32CEECA534A9C6) ist schwieriger zu faken, aber auch nicht als kryptografisch sichere ID entworfen.
4. Am besten ist es, wenn man den gesuchten Schlüssel anhand des Fingerprint sucht (zB. 0x68995C53D2CEE11B0E4182F62146D0CD2B3CAA3E). Diese Suche liefert als einzige Variante vertrauenswürdige Ergebnisse.

Keyserver Konfiguration für GnuPG 2.1

Wenn man GnuPG Verion 2.1 verwendet, dann werden die Keyserver in der Konfigurationsdatei *$HOME/.gnupg/dirmngr.conf* bzw. *%APPDATA%/GnuPG/dirmngr.conf* konfiguriert.

Man kann zwei Keyserver angeben, einen HKP(S)-Keyserver und einen Tor Hidden Service (siehe: Kapitel Anonymisierungsdienste). Wenn ein Tor Onion Router läuft, dann wird der Tor Hidden Service verwendet, anderenfalls wird der HKP(S) Keyserver gefragt.

Wenn man SSL/TLS-Verschlüsselung für den Keyserver Pool verwenden möchte, dann muss man außerdem das CA-Root Zertifikat *sks-keyservers.netCA.pem*[16] herunter laden und in der Konfiguration eintragen:

```
keyserver hkp://jirk5u4osbsr34t5.onion
keyserver hkps://hkps.pool.sks-keyservers.net

hkp-cacert <Path to>/sks-keyservers.netCA.pem
```

Die automatische Umschaltung zwischen HKP(S) Keyserver und Tor Hidden Service erfolgt nur bei der Suche auf der Kommandozeile. Grafische GUIs zur Schlüsselverwaltung wie z.B. Enigmail oder GPA erzwingen die Verwendung des jeweils konfigurierten Keyservers.

SSL-Verschlüsselung für Keyserver mit GnuPG 2.0

Seit Anfang Oktober 2012 bietet der Keyserverpool sks-keyservers.net einen Sub-Pool mit SSL-Verschlüsselung für das Abrufen und Senden von OpenPGP-Schlüsseln [17]. Die SSL-Verschlüsselung verhindert, dass ein Lauscher beobachtet, welche OpenPGP-Schlüssel man sucht und herunter lädt.

Um diesen sicheren Sub-Pool zu nutzen, sind folgende Schritte nötig:

1. Man benötigt eine Version von GnuPG, die das *hkps://* Protokoll unterstützt. Man kann *gnupg2* nutzen oder das Paket *gnupg-curl* installieren.
2. Das CA-Root Zertifikat des Keyserverpool *sks-keyservers.netCA.pem*[18] ist herunter zu laden und auf dem eigenen Rechner zu speichern.
3. Damit man die SSL-verschlüsselten Keyserver auch mit den Kommandozeiletool *gnupg2* nutzen kann, kann man in der Konfigurationsdatei *gpg.conf* folgende Parameter setzen:

[16] https://sks-keyservers.net/sks-keyservers.netCA.pem
[17] http://permalink.gmane.org/gmane.comp.encryption.pgp.sks/3559
[18] https://sks-keyservers.net/sks-keyservers.netCA.pem

```
keyserver hkps://hkps.pool.sks-keyservers.net
keyserver-options ca-cert-file=<Path to>/sks-keyservers.netCA.pem,...
```

4. Wer es vermeiden möchte, eine Konfigurationsdatei mit einem Editor anzupassen, kann in der Konfiguration von Enigmail die *Experten Optionen* aktivieren und folgende Werte eintragen:

   (a) Auf dem Reiter *Schlüssel-Server* ist der HKPS-Pool als Schlüssel-Server einzutragen:

   ```
   hkps://hkps.pool.sks-keyservers.net
   ```

   (b) Auf dem Reiter *Erweitert* muss man als *Zusätzliche Parameter für GnuPG* die Keyserver-Option für das *ca-cert-file* ergänzen:

   ```
   --keyserver-options ca-cert-file=<Path to>/sks-keyservers.netCA.pem
   ```

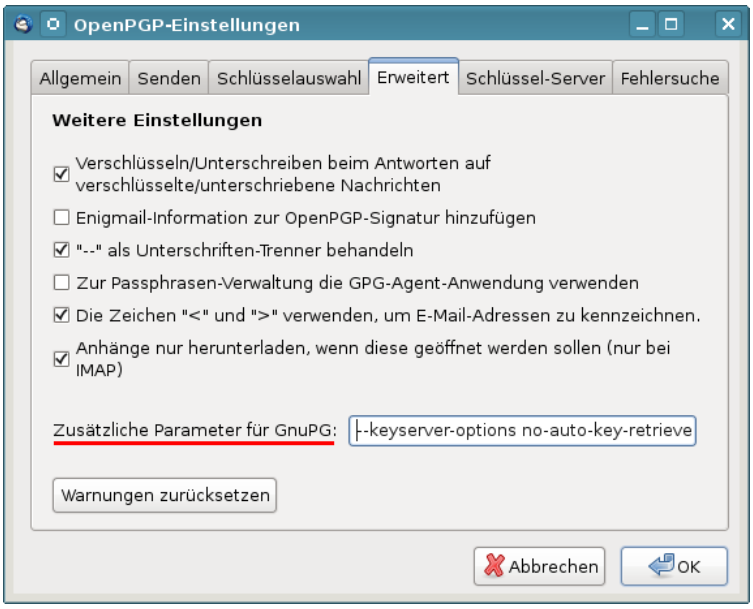


Abbildung 7.10: Keyserver Optionen in Enigmail eintragen

7.1.11 Mailvelope Browser Add-on

Mailvelope ist ein Add-on für die Browser Mozilla Firefox und Google Chrome, das OpenPGP Verschlüsselung im Webinterface bietet und immer populärer wird. Es wird von WEB.de, GMX.de und Posteo.de als sichere Lösung für Ende-zu-Ende Verschlüsselung im Browser beworben und auch vom BSI empfohlen. (Hmmm - das BSI hat manchmal seltsame Empfehlungen.)

Mailvelope hat konzeptuell bedingt einige Schwächen in der Sicherheit und bietet nur *hinreichende Sicherheit*. Auch der Hauptentwickler von Mailvelope stimmt darin überein, dass Mailvelope für hohe Sicherheitsanforderungen nicht geeignet ist.

Konzeptuell hat Mailvelope folgende Schwächen:

- **Unsichere Speicherung der Schlüssel:** Die Schlüssel werden im HTML5 Storage des Browsers gespeichert. Im HTML5 Security Cheat Sheet wird vom OWASP empfohlen, keine sensitiven Informationen im Local Storage des Browsers zu speichern, da diese Daten mit XSS-Angriffen kompromittiert werden könnten. Auch die Security Analyse zu Mailvelope (PDF) weist auf das Risiko von XSS-Angriffe hin, obwohl die Entwickler sich bemühen, das Risiko zu reduzieren.

  Hinweis: Um bei Nutzung von Mailvelope in Firefox das Risiko von XSS-Angriffen zu verringern, sollte man unbedingt das Add-on NoScript zusätzlich installieren, da Firefox keinen XSS-Schutz enthält.

- **Javascript ist nicht für starke Krypto geeignet:** Javascript wurde nicht als Programmiersprache für Krypto-Anwendungen entworfen. Best Practices für die Implementierung von Krypto sind mit Javascript nicht umsetzbar, einige Beispiele:

  - Javascript bietet keine Möglichkeiten, bei der Programmierung identische Ausführungszeiten für Code Verzweigungen zu erzwingen. Duch Seitenkanalangriffe ist es damit möglich, die Reihenfolge der Nullen und Einsen im privaten Schlüssel durch Beobachtung bei der Codeausführung zu rekonstruieren. In modernen Krypto-Bibliotheken ist das ein Securitybug (z.B. CVE-2016-7056 ECDSA P-256 timing attack key recovery, OpenSSL).

    Seitenkanalangriffe auf Browser sind einfach, da der Rechner nicht kompromittiert werden muss. Das Script für den Angriff kann von einer beliebigen Webseite geladen werden, wie Forscher in dem Paper *The Spy in the Sandbox – Practical Cache Attacks in Javascript* gezeigt haben.
  - Mit Javascript is es nicht möglich, einen geheimen Schlüssel nach der Benutzung aus dem Hauptspeicher zu löschen (Overwriting memory - why?). Das normale Verhalten von Mailvelope wurde bei Tor Onion Router als Security Bug eingestuft.[19]

  Was in anderen Krypto-Implementierungen als schwerer Bug gilt, wird bei Mailvelope einfach als Javascript Limitierung hingenommen.

- **Zugriff auf private Schlüssel durch E-Mail Provider:** Mit Zustimmung des Nutzers hat der E-Mail Provider über die API Zugriff auf die privaten OpenPGP Schlüssel. Web.de und GMX.de bewerben dieses Feature für die Synchronisation zwischen den Browsern, bei mailbox.org

[19] https://heise.de/-1746523

dient es als Backup... das BSI hat keine Einwände dagegen. Die privaten Schlüssel werden an den E-Mail Provider nur mit einem extra Passwort verschlüsselt übertragen, trotzdem ist dieser Zugriff bedenklich.

Diese Funktion zum Zugriff auf den privaten Schlüssel wird insbesondere dann bedenklich, wenn das Mailvelope Add-on vom E-Mail Provider bereitgestellt wird, wie bei Web.de und GMX.de. Besser ist es, das Add-on aus einer vertrauenswürdigen, unabhängigen Quelle zu installieren.

Hier im Privacy-Handbuch empfehlen wir deshalb, für die Ende-zu-Ende Verschlüsselung einen E-Mail Client mit GnuPG Support zu nutzen. Diese Lösung ist für hohe Sicherheitsanforderungen geeigent. Wer höchste Sicherheitsanforderungen braucht, der sollte außerdem eine OpenPGP Smartcard für den privaten Schlüssel verwenden, um eine Kompromittierung auch bei gezielten Angriffen zu vermeiden. Außerdem empfehlen wir u.a. aus Sicherheitsgründen, grundsätzlich eine E-Mail Client zu bevorzugen, statt die E-Mails im Webinterface des Providers zu verwalten.

7.1.12 OpenPGP-Verschlüsselung für Kontaktformulare

Das Metadaten (z.B. Absender und Empfänger einer E-Mail) für die Überwachung eine große Rolle spielen, ist seit den Veröffentlichungen von Snowden/Greenwald allgm. bekannt. Leser des Privacy-Handbuches haben es evtl. vorher gewusst (siehe: Kommunikationsanalyse).

Kontaktformulare bieten eine Möglichkeit, diese Metadaten zu verschleiern. Wer ein Blog oder eine Webseite betreibt, kann recht einfach ein Kontaktformular zur Verfügung stellen. Es gibt Wordpress Plug-ins für Kontaktformulare, einfache PHP-Scripte oder fertige Perl-CGI Scripte. Man kann eine individuell passende Lösung wählen. Dabei sollte man auf folgendes achten:

1. Das Kontaktformular sollte den Absender nicht zur Eingabe seiner E-Mail Adresse zwingen. Als work-around kann man im HTML-Code des Formulares das Feld für die Absender E-Mail Adresse als *hidden* deklarieren und einen Standardwert setzen.

2. Das Script sollte die IP-Adresse des Absenders nicht in den Header der E-Mail einfügen. Einige Scripte für Kontaktformulare wollen damit den Spam-Schutz verbessern. Einfach ausprobieren.

3. Das Kontaktformular sollte immer via HTTPS (SSL-verschlüsselt) aufgerufen werden. Wenn die Webseite auch via plain HTTP erreichbar ist, sollten alle Links auf der Webseite zum Kontaktformular mit der vollständigen URL angegeben werden:

   ```
   <a href="https://www.server.tld/kontakt.html">Kontakt</a>
   ```

   Jeder gute Webhoster bietet inzwischen SSL-Verschlüsselung für einen kleinen Aufpreis für alle Kunden, Wordpress.com hat es standardmäßig für alle Kunden aktiviert.

Im folgenden möchte ich einige Möglichkeiten vorstellen, wie man ein Kontaktformular mit OpenPGP-Verschlüsselung aufmotzen könnte.

Hinweis: Bei allen Varianten handelt es nich um *server based crypto*, die nicht die gleiche Sicherheit wie richtige Ende-zu-Ende Verschlüsselung gewährleisten kann.

Ganz einfach ohne Programmierung

Man kann einen guten E-Mail Provider nutzen, der TLS-Verschlüsselung für eingehende E-Mails erzwingen kann und ein verschlüsseltes Postfach bietet, z.B. mailbox.org.

- Nachdem man einen E-Mail Account bei mailbox.org erstellt und bezahlt hat, ist der Alias für TLS-verschlüsselten Versand/Empfang zu aktivieren sowie das OpenPGP verschlüsselte Postfach zu aktivieren und der eigene OpenPGP public Key hochzuladen.
- Im Script des Kontaktformulares konfiguriert man als Empfänger die E-Mail Adresse *<name>@secure.mailbox.org* bzw. *<name>@tls.mailbox.org*.

Vom Browser des Absenders wird die Nachricht SSL-verschlüsselt zum Webserver übertragen. Von dort wird sie über eine TLS-verschlüsselte Verbindung an Mailbox.org gesendet und auf dem Mailserver mit dem OpenPGP-Key verschlüsselt.

Diese Variante schützt den Inhalt der Nachrichten gegen den allgmeinen Überwachungswahn und bei Beschlagnahmung von Daten. Sie schützt nicht gegen eine TKÜ nach §100 a/b StPO beim Hoster des Kontaktformulars oder beim E-Mail Provider, da der Inhalt als Plain-Text an diesen Stellen mitgelesen werden kann.

Mit Javascript im Browser des Absenders

Diese Variante erfordert HTML-Kenntnisse, um einige Anpassungen im HTML-Code des Kontaktformulares vorzunehmen und die Bibliothek *OpenPGPjs* einzubinden.

Hinweis: Verschlüsselung mit Javascript im Browser bietet keine hohe Sicherheit, lediglich hinreichende Sicherheit. Die Gründe wurden bereits mehrfach erwähnt. Für den Erstkontakt ist es aber besser als unverschlüsselt.

1. Die aktuelle Version der Bibliothek *openpgp.min.js* von der Projektwebseite https://github.com/openpgpjs/openpgpjs/releases herunter laden und auf den eigenen Webserver kopieren.
2. Das Javascript Schnipselchen *encrypt_message.js* von meiner Webseite https://www.privacy-handbuch.de/handbuch_32v.htm herunter laden und auf den Webserver kopieren. Dieses Javascript Schnipselchen verschlüsselt das Textarea Feld mit der ID textitmessage. Wenn das Textarea im Formular eine andere ID hat, ist die Zeilen 3 anzupassen:

```
var message = document.getElementById("message");
```

3. Im HTML-Header der Webseite des Formulares sind die Scripte zu laden:

```
...
<script src="/openpgp.min.js" type="text/javascript">
<script src="/encrypt_message.js" type="text/javascript">
...
```

4. Im HTML-Code des Formulares im FORM-Tag die Funktion *encrypt_message()* als *onsubmit*-Tag hinzufügen, so dass die Funktion automatisch beim Versand der Daten ausgeführt wird und zuerst das Textfeld mit der ID *message* verschlüsselt:

```
<FORM name="contact" method="post" action="https://server.tld/...."
   onsubmit="return encrypt_message();">

<textarea id="message" ...> </textarea>

</form>
```

5. Außerdem ist der eigenen OpenPGP public Key als versteckter DIV-Container mit der ID *pubkey* im HTML-Code einzubauen.

```
<div id="pubkey" hidden="true">
-----BEGIN PGP PUBLIC KEY BLOCK-----
....
-----END PGP PUBLIC KEY BLOCK-----
</div>
```

6. Für Surfer, die Javascript standardmäßig deaktivieren kann man ein Hinweis einfügen, dass Javascript für die Funktion des Formulares nötig ist:

```
<NOSCRIPT>
Bitte aktivieren Sie Javascript für die Verschlüsselung der Nachricht!
</NOSCRIPT>
```

Hinweise: Einige ältere Browser können keine krypto-tauglichen Zufallszahlen mit Javascript erzeugen. Das kann die Verschlüsselung deutlich schwächen. Deshalb ist es mit diesen Browsern nicht möglich, das Formular zu nutzen. Außerdem kann die Verschlüsselung auf dem Server durch unbemerkte Modifikationen am Javascript Code angegriffen werden. Trotzdem ist es besser, als keine Verschlüsselung zu verwenden.

7.1.13 Web des Vertrauens

Im Prinzip kann jeder Anwender einen Schlüssel mit beliebigen E-Mail Adressen generieren. Um Vertrauen zu schaffen, gibt es das **Web of Trust**.

Hat Beatrice die Echtheit des Schlüssels von Anton überprüft, kann sie diesen mit ihrem geheimen Schlüssel signieren und auf die Schlüsselserver

re-exportieren. Conrad, der den Schlüssel von Beatrice bereits überprüft hat, kann damit aufgrund der Signatur auch dem Schlüssel von Anton vertrauen. Es bildet sich ein weltweites Netz von Vertrauensbeziehungen. Die Grafik Bild 7.11 zeigt eine mögliche Variante für den Key von Anton (A).

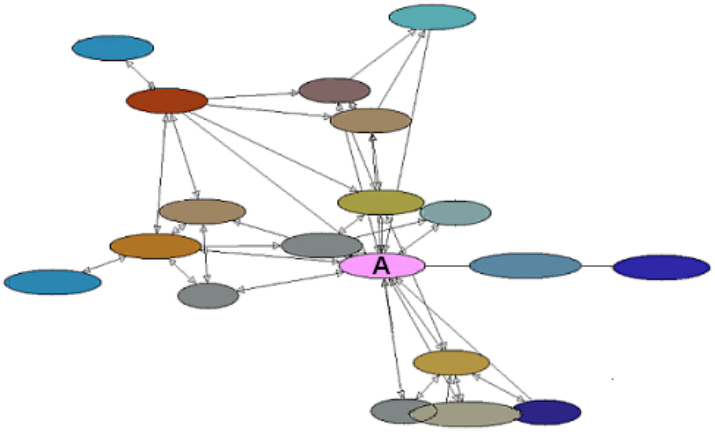


Abbildung 7.11: Beispiel für ein Web of Trust

OpenPGP-Schlüssel signieren

Die Echtheit eines Schlüssels kann anhand des Fingerabdrucks geprüft werden. Zu jedem Schlüssel existiert ein eindeutiger Fingerabdruck. Dieser lässt sich in den Eigenschaften des Schlüssels anzeigen. In der Schlüsselverwaltung ist der zu prüfende Schlüssel auszuwählen und über den Menüpunkt *Anzeigen - Eigenschaften* den im Bild 7.12 dargestellten Dialog zu öffnen.

Der angezeigte Fingerabdruck des Schlüssels kann mit dem Wert verglichen werden, den man vom Eigentümer des Schlüssels erhalten hat. Sind beide identisch, kann das Vertrauen des öffentlichen Schlüssels auf ein hohes Niveau gesetzt werden. Den Dialog findet man in der Schlüsselverwaltung unter *Bearbeiten - Vertrauenswürdigkeit*.

Hat man sich von der Echtheit des Schlüssels überzeugt, kann man ihn in Absprache mit dem Schlüsseleigentümer auch signieren und den signierten Schlüssel auf einen Keyserver exportieren. Wenn viele Nutzer die Ergbnisse ihrer Überprüfung online verfügbar machen, entsteht das Web-of-Trust und es wird schwer, gefälschte Schlüssel in Umlauf zu bringen.

Certification Authorities

Diese Infrastruktur kann auch von vertrauenswürdigen Institutionen (Certification Authorities, CAs) genutzt werden. Die Nutzer wenden sich an die CA und lassen gegen Vorlage von Ausweisdokumenten den eigenen

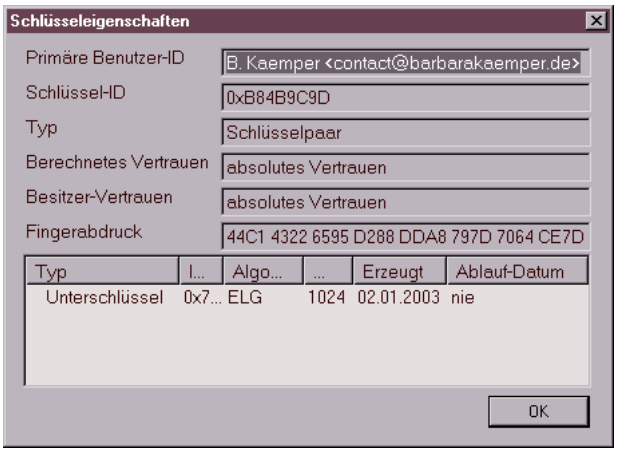


Abbildung 7.12: Schlüssel-Eigenschaften

OpenPGP-Key signieren. Alle Partner benötigen lediglich den öffentlichen Schlüssel der CA, um die Echtheit der Schlüssel zu überprüfen.

Beispiele für Certification Authorities sind:

- CAcert.org signiert auch OpenPGP-Schlüssel
- Krypto-Kampagne der Zeitschrift c't
- PCA des Deutschen Forschungsnetzes (DFN-PCA)

Keysigning-Party

Wenn sich mehrere OpenPGP-Nutzer treffen um sich gegenseitig die Echtheit ihrer Schlüssel zu bestätigen, nennt man es eine *Keysigning-Party*. Dabei kommt es nicht darauf an, dass die Beteiligten sich persönlich kennen. Die Echtheit des Schlüssels können auch Unbekannte gegen Vorlage von Ausweisdokumenten und Fingerprint des Key bestätigen.

Eine Keysigning-Party läuft üblicherweise folgendermaßen ab:

1. Der Organisator lädt zu einer Party ein und bittet um Anmeldungen.
2. Wer an der Party teilnehmen möchte, sendet seinen public OpenPGP-Key zusammen mit Namen und dem Fingerprint an den Organisator.
3. In Vorbereitung der Party erstellt der Organisator einen Keyring für alle Beteiligte und eine Liste mit Namen, Key-IDs und Fingerprints von allen Teilnehmern.
4. Der Keyring und die Liste werden an alle Teilnehmer verteilt. Die Teilnehmer können auf der Party die Identität gegenseitig durch Vorlage von Ausweisdokumenten prüfen.

5. Wieder zuhause können die Schlüssel im Party-Keyring signiert und an die Inhaber per E-Mail versendet werden. In der Regel erfolgt dieser Schritt nicht beim Treffen.

Wer häufiger an Keysigning-Partys teilnimmt, kann unter Linux das Tool *caff* für den letzten Schritt nutzen. Das Tool ist im Paket *signing-party* für nahezu alle Linux-Ditributionen verfügbar und kann mit dem Paket-Manager der Wahl installiert werden.

Nach der Installation ist die Datei $HOME/.caffrc als Textdatei anzulegen und die Werte für den eigenen Namen, E-Mail Adresse, OpenPGP-ID sowie die Parameter zur Versendung von E-Mails sind zu konfigurieren:

```
$CONFIG{'owner'} = 'Michi Müller';
$CONFIG{'email'} = 'm@m.de';
$CONFIG{'keyid'} = [ qw{01234567890ABCDE} ];

$CONFIG{'mailer-send'} =  [ 'smtp', Server => 'mail.server', Auth => ['user','pass'] ];
```

Ein kleines Kommando im Terminal signiert alle Schlüssel des Party-Keyring, verpackt sie in E-Mails, die mit dem Key der Empfänger verschlüsselt werden, und sendet die E-Mails an die Inhaber der OpenPGP-Keys:

```
> caff --key-file party-keyring.asc
```

7.1.14 Schlüssel zurückrufen

Soll ein Schlüsselpaar nicht mehr verwendet werden (beispielsweise weil der geheime Schlüssel kompromittiert wurde oder die Passphrase in Vergessenheit gefallen ist), kann der öffentliche Schlüssel für ungültig erklärt werden.

Öffnen Sie die Schlüsselverwaltung, wählen Sie den Schlüssel, der für ungültig erklärt werden soll. Rufen Sie den Menüpunkt *Bearbeiten / zurückrufen* auf. Nach einer Sicherheitsfrage und Eingabe der Passphrase wird der Schlüssel auf den Schlüsselservern im Internet für ungültig erklärt. Auch wenn der geheime Schlüssel nicht mehr vorliegt oder die Passphrase in Vergessenheit geraten ist, kann der öffentliche Schlüssel für ungültig erklärt werden, indem das unter Punkt 4 erstellte Rückrufzertifikat importiert wird.

7.2 S/MIME mit Thunderbird

S/MIME nutzt Zertifikate nach dem Standard X.509 für die Verschlüsselung und Signatur von E-Mails. Eine *Certification Authority* (CA) bestätigt mit einer Signatur die Echtheit und die Identität des Besitzers eines ausgegebenen Zertifikates. Für diese Signatur wird das *Root Certificate* der CA genutzt. Die Root Certificates etablierter CAs sind in nahezu allen Browsern und E-Mail Clients enthalten. Wer diesen Zertifikaten vertraut, vertraut auch ohne weitere Nachfrage den damit signierten persönlichen Zertifikaten anderer Nutzer.

7.2.1 Kostenfreie Certification Authorities

In der Regel kostet dieser Service bei einer etablierten CA 30-100 Euro pro Jahr. **CAcert.org** bietet eine kostenfreie Alternative für die Ausstellung und Signatur von X.509 Zertifikaten. CAcert.org ist ein *Web of Trust* von Nutzern, welche sich gegenseitig bei einem persönlichen Treffen die Identität bestätigen. Einfache Nutzer werden durch Assurer verifiziert, die ehrenamtlich für CAcert.org arbeiten.

Für jede Bestätigung durch einen Assurer erhält der Nutzer bis zu 35 Punkte. Sobald man 50 Punkte angesammelt hat, also nach mindestens 2 unabhängigen Bestätigungen, kann man sich auf der Website ein Class-3 Zertifikat mit dem eigenen Namen generieren. Mit einem Punktestand von 100 Punkten kann man den Status eines Assurers beantragen.

Auch ohne Bestätigungen durch Assurer kann man ein Zertifikat zu erzeugen. Dieses Class-1 Zertifikat enthält nur die E-Mail Adresse des Besitzers und keinen verifizierten Namen.

Der Weg zur Erstellung eines S/MIME-Zertifikates:

- Wer häufig CAcert.org nutzt, sollte das Root-Zertifikat dieser CA in den Browser importieren. Man erspart sich damit lästige Nachfragen beim Besuch der Website. Die Root Zertifikate von CAcert.org ist standardmäßig nicht in den häufig genutzten Browsern enthalten. CAcert.org bietet sie auf der Webseite zum Download.

- Es ist notwendig, die Root-Zertifikate von CAcert.org in den E-Mail Client als vertrauenswürdige CA zu importieren. Nur so kann die Gültigkeit des eigenen Zertifikates überprüft werden.

- Die Anmeldung folgt dem üblichen Schema. Nach Eingabe der Kontaktdaten erhält man eine E-Mail zu Verifizierung und kann sich im Anschluss auf der Website einloggen, um die persönlichen Angaben zu vervollständigen.

- Zur Bestätigung der Identität kann man auf der Website einen Assurer in der Nähe suchen und um ein persönliches Treffen bitten. Zum Treffen ist ein Ausdruck des WOT-Formulars für den Assurer mitzubringen.

- Hat man 50 Punkte durch Bestätigungen von mehreren Assurer erreicht, kann man auf der Webseite ein Zertifikat erstellen. Das Zertifikat und den Privaten Key findet man nach dem Vorgang in der Zertifikatsverwaltung des Browsers unter *Eigene Zertifikate*! Es gibt keinen Downloadlink o.ä.
- Das Zertifikat wird aus der Zertifikatsverwaltung des Browsers als *.P12 Datei exportiert und im E-Mail Client wieder importiert.

7.2.2 Erzeugen eines Zertifikates

Die verschiedenen Certification Authoroties (CAs) bieten ein Webinterface, um nach der Überprüfung der Identität ein signiertes Zertifikat zu erstellen. In der Regel stehen zwei Wege zur Auswahl:

1. Die CA führt den kompletten Vorgang auf einer Webseite aus: die Generierung des privaten Schlüssels inklusive Sicherung mit einer Passphrase, die Generierung des Certification Request (CSR), die Signierung des CSR und die Erstellung der Zertifikatsdatei mit privatem und öffentlichem Schlüssel.
2. Der Anwender erstellt den privaten Schlüssel und den Certification Request (CSR) selbst. Dann wird nur der CSR mit dem öffentlichen Schlüssel zum Server der CA geladen, dort signiert und als signiertes Zertifikat nach Prüfung der Identität von der CA zum Download bereitgestellt. Der private Schlüssel verlässt dabei nie den Rechner des Nutzers.

Da die Sicherheit asymmetrischer Verschlüsselung davon abhängt, dass nur der Anwender Zugriff auf den privaten Schlüssel hat, sollte man sich die Mühe machen und den zweiten Weg gehen. Anderenfalls ist es möglich, dass der private Schlüssel bereits vor der ersten Verwendung kompromittiert wird. Man kann den Certification Authorithies nicht blind vertrauen.

Schrittweise Anleitung für die Kommandozeile

Die OpenSSL-Bibliothek bietet alles Nötige. Die Tools sind unter Linux installiert.

1. Generieren eines passwortgeschützten privaten Schlüssels in der Datei *mein.key*:

   ```
   > openssl genrsa -out mein.key -des3 4096
   ```

2. Generieren eines Certification Request (CSR) in der Datei *mein.csr*, die folgenden Daten werden dabei abgefragt:

   ```
   > openssl req -new -key mein.key -out mein.csr
   Enter pass phrase for mein.key:
   ....
   Country Name (2 letter code) [AU]: DE
   State or Province Name (full name) []: Berlin
   Locality Name (eg, city) []: Berlin
   Organization Name (eg, company) []: privat
   ```

```
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []: Max Musterman
Email Address []: max@musterman.de
```

3. en CSR übergibt man der CA. Die Datei enthält nur den öffentlichen Schlüssel. Die CA signiert diesen CSR und man erhält ein signiertes Zertifikat als Datei *mein.crt* via E-Mail oder als Download Link.

4. Diese Datei kann man an alle Kommunikationspartner verteilen.

5. Für den Import im eigenen E-Mail Client fügt man privaten Schlüssel und signiertes Zertifikat zu einer PKCS12-Datei *mein.p12* zusammen.

   ```
   > openssl pkcs12 -export -in mein.crt -inkey mein.key -out mein.p12
   ```

   Diese passwortgeschützte Datei kann in allen E-Mail Clients importiert werden und sollte sicher verwahrt werden.

7.2.3 S/MIME-Krypto-Funktionen aktivieren

Liegt eine Datei mit signiertem Zertifikat und geheimem Schlüssel vor, können die S/MIME-Funktionen für ein E-Mail Konto aktiviert werden. Es ist der Dialog mit den Konto-Einstellungen zu öffnen und in die Sektion *S/MIME-Sicherheit* zu wechseln (Bild 7.13).

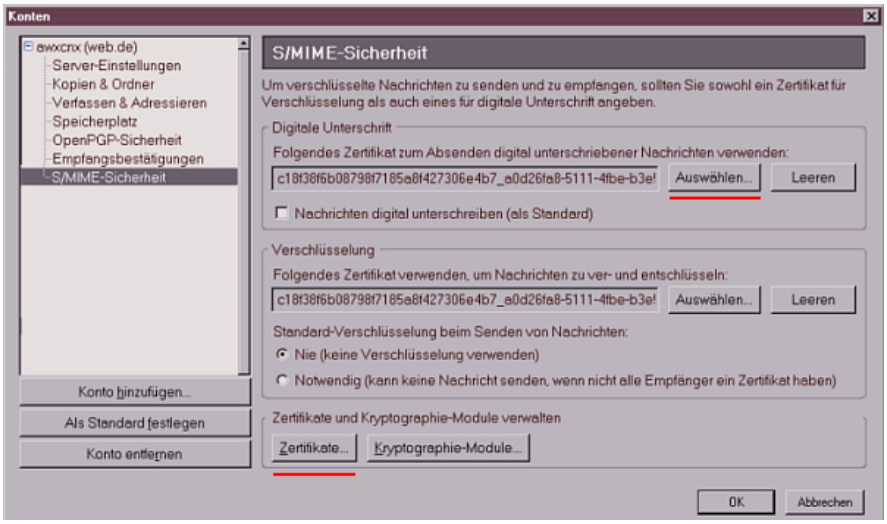


Abbildung 7.13: Kontoeinstellungen zur S/MIME-Sicherheit

Zuerst ist das persönliche Zertifikat zu importieren. Ein Klick auf den Button *Zertifikate* öffnet den Manager für eigene Zertifikate (Bild 7.14). Hier ist der Button *Importieren* zu wählen und das gespeicherte persönliche Zertifikat mit öffentlichem und geheimem Schlüssel zu importieren.

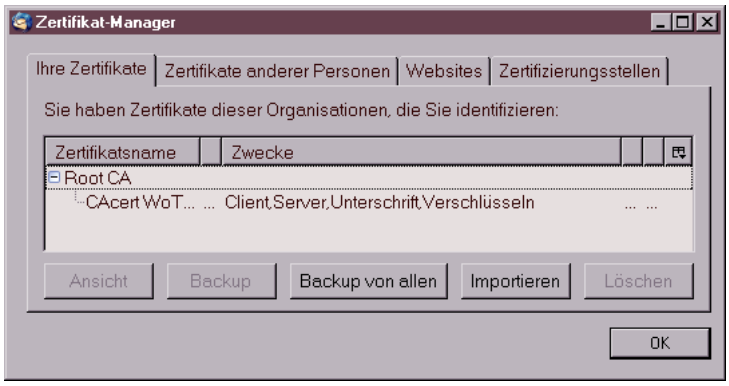


Abbildung 7.14: Zertifikatsmanager für eigene Zertifikate

Es folgt eine Abfrage des Passwortes, mit dem der Zugriff auf den geheimen Schlüssel geschützt werden soll und evtl. die Frage nach dem Passwort, mit welchem die Datei verschlüsselt wurde. Der Zertifikatsmanager ist im Anschluss mit einem Klick auf den Button *Ok* zu schließen und in den Konto-Einstellungen das frisch importierte Zertifikat für das Signieren und Entschlüsseln auszuwählen.

Sollen alle ausgehenden Nachrichten standardmäßig signiert werden, kann die entsprechende Option aktiviert werden.

Thunderbird bietet die Möglichkeit, das Online Certifate Status Protocol (OCSP) für die Validierung von Zertifikaten zu nutzen. Standardmäßig ist die Nutzung dieser Funktion sinnvoll deaktiviert. Da nur validierte Zertifikate für die Verschlüsselung und Signaturprüfung genutzt werden können, muss man das Root Zertifikat der ausstellenden CA von der Website herunterladen und importieren. Dies kann vereinfacht werden, wenn man im Dialog *Einstellungen* in der Sektion *Datenschutz* auf dem Reiter *Sicherheit* den Button *OCSP...* wählt und die Option *OCSP verwenden* aktiviert. Damit hat man jedoch keine Möglichkeit zu entscheiden, ob man der CA wirklich vertraut.

7.2.4 Zertifikate der Partner und der CA importieren

Im Gegensatz zu OpenPGP, das im Internet eine ausgereifte Infrastruktur zur Verteilung öffentlicher Schlüssel bereitstellt, muss der Inhaber eines S/MIME-Zertifikates selbst die Verteilung übernehmen. Am einfachsten ist es, dem Partner eine signierte E-Mail zu senden. Alle E-Mail Clients mit S/MIME Support können aus der Signatur das Zertifikat importieren und tun dies in der Regel ohne Nachfrage.

Bevor der Empfänger einer signierten E-Mail die Signatur prüfen und verschlüsselt antworten kann, muss er das Zertifikat verifizieren. Viele Root-Zertifikate sind bereits in gängigen E-Mail Clients enthalten. Einige muss der Nutzer jedoch erst selbst importieren. Diese Root-Zertifikate stehen auf

den Websites der Ausstellers zum Download bereit. Wurde die Gültigkeit verifiziert, kann der Empfänger im Anschluß verschlüsselt antworten.

Es ist auch möglich, eine Datei nur mit dem öffentlichen Schlüssel des Zertifikates auf den Rechner des Partners zu transferieren. Dort ist die Datei in Thunderbird zu importieren.

Für den Import eines Zertifikates in Thunderbird ist der Dialog *Einstellungen* zu öffnen. In der Sektion *Datenschutz* auf dem Reiter *Sicherheit* ist der Button *Zertifikate* zu wählen (Bild 7.15), um die Verwaltung zu öffnen.

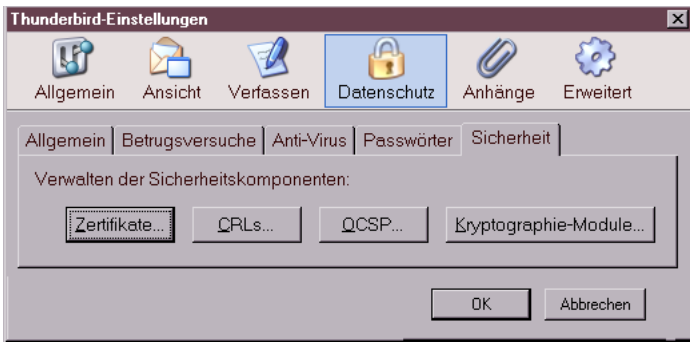


Abbildung 7.15: Dialog Sicherheits-Einstellungen

Im Zertifikatsmanager ist auf dem Reiter *Zertifikate anderer Personen* der Button *Importieren* zu finden, welcher eine Dateiauswahl öffnet, um das erhaltene Zertifikat aus einer lokal gespeicherten Datei zu importieren.

Die Root-Zertifikate weiterer Certification Authorities (CAs) können auf dem Reiter *Zertifizierungsstellen* importiert werden.

7.2.5 Nachrichten verschlüsseln und signieren

Wenn das persönliche Zertifikat bestehend aus öffentlichem und geheimem Schlüssel importiert wurde, ist es möglich, signierte E-Mails zu versenden. Wurden Zertifikate mit den öffentlichen Schlüsseln der Kommunikationspartner importiert, kann die Nachricht auch verschlüsselt werden.

Für die Wahl der Optionen steht im Editor einer neuen Nachricht der Button S/MIME zur Verfügung. Klickt man auf den kleinen schwarzen Pfeil unmittelbar neben dem Button S/MIME, öffnet sich das im Bild 7.16 dargestellte Menü zum Festlegen der Kryptographie-Optionen für die aktuelle Nachricht.

Eine Möglichkeit, für bestimmte Empfänger die Einstellungen für Verschlüsselung dauerhaft festzulegen, bietet Thunderbird in der Standard-Konfiguration nicht. Man muß bei jeder neu verfassten E-Mail daran denken,

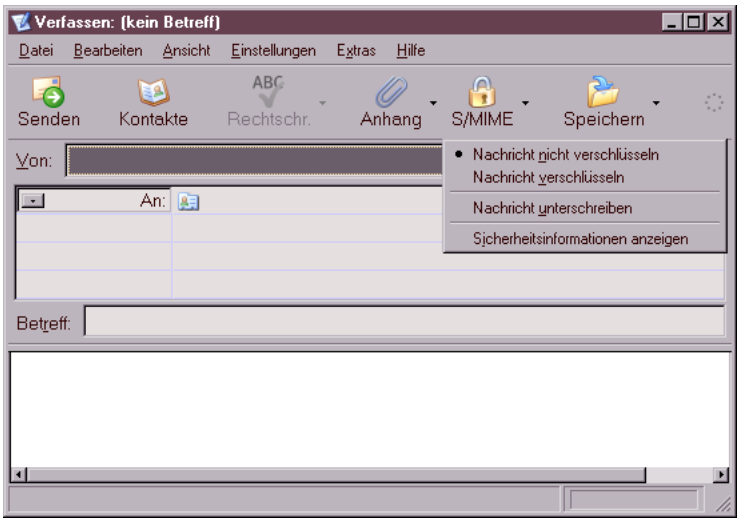


Abbildung 7.16: Verschlüsseln oder Signieren einer E-Mail

sie wenn möglich zu verschlüsseln! Das ist sehr fehleranfällig.

Eine Lösung bietet das Plug-In **Virtual Identity**. Es kann bei jeder versendeten E-Mail die gewählten Einstellungen für die Verschlüsselung speichern. Damit lernt Thunderbird, welche Verschlüsselungseinstellungen für welche Empfänger gelten. Die Einstellungen werden bei jeder neuen E-Mail an den Empfänger als Default aktiviert.

Nach der Installation des Plug-Ins muss man unter dem Menüpunkt *"Extras - Virtual Identity - Einstellungen"* die Speicherung der Einstellungen für die Verschlüsselung aktivieren. (Bild 7.17)

Unter dem Menüpunkt *"Extras - Virtual Identity - Datenspeicher"* findet man die gesammelten Daten und kann sie auch editieren.

7.2.6 Root-Zertifikate importieren

Das Importieren der Zertifikate in Web-Browser und E-Mail-Client erspart lästige Nachfragen, ob man einem mit diesem Root-Zertifikat signierten Zertifikat vertrauen möchte.

Webbrowser Firefox

Nutzer des Browsers Firefox klicken auf auf das *Root Certificate* und aktivieren in dem sich öffnenden Dialog (Bild 7.18) mindestens den ersten und zweiten Punkt.

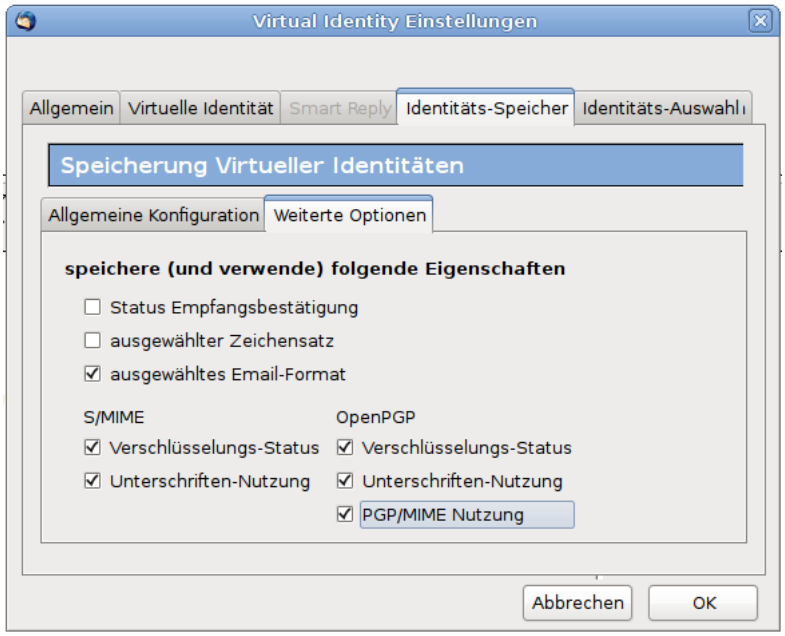


Abbildung 7.17: Einstellungen des Plug-In Virtual Identity

E-Mail-Client Thunderbird

Für den Import der Root-Zertifikate in den E-Mail-Client sind diese lokal zu speichern. In der Regel benötigt man neben dem *Class 1 Root Certificate* auch das *Class 3 Root Certificate*, da mit diesem Unterzertifikat die E-Mail-Zertifikate der Nutzer signiert werden. Nutzer des Browsers Firefox klicken mit der rechten Maustaste auf den Link und wählen aus dem Kontextmenü den Punkt *Ziel speichern unter ...*

Anschließend ist Thunderbird zu starten und der Dialog *Einstellungen* zu öffnen. In der Sektion *Datenschutz / Sicherheit* ist der Button *Zertifikate* zu wählen, um den in Bild 7.19 dargestellten Manager für Zertifikate zu öffnen.

In diesem Dialog ist auf dem Reiter *Zertifizierungsstellen* der Button *Importieren* zu wählen und das zuvor gespeicherte Zertifikat zu importieren. Im Anschluss sind im folgenden Dialog mindestens die ersten beiden Optionen zu aktivieren (siehe Firefox).

7.2.7 Eine eigene Certification Authority

Wer eine eigene Certification Authority (CA) betreiben möchte, benötigt etwas Erfahrung, einige kleine Tools und ein paar Byte Webspace, um das eigene Root-Zertifikate, die Revocation List und die Policy der CA dort zum Download bereitzustellen.

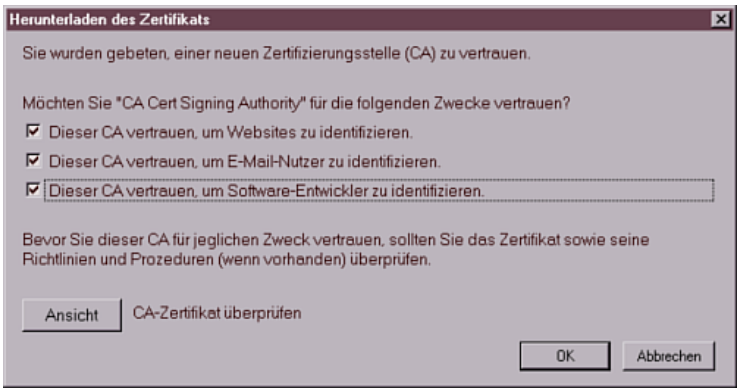


Abbildung 7.18: Herunterladen eines Zertifikates

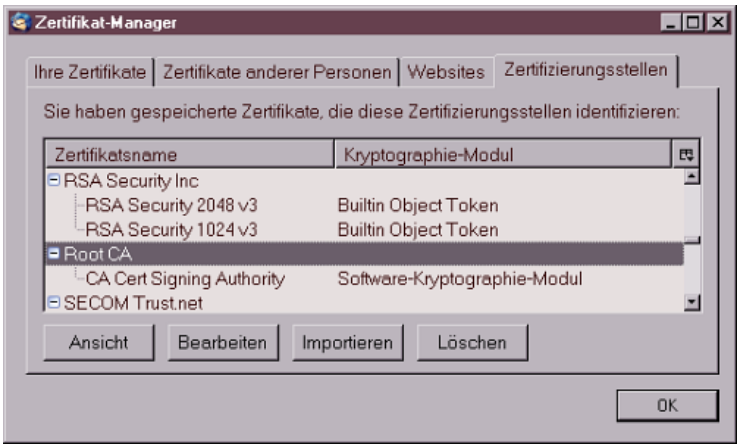


Abbildung 7.19: Zertifikats-Manager von Thunderbird

Die OpenSSL-Bibliothek enthält alle nötigen Funktionen, um eine eigene CA zu verwalten. Die Hardcore Version auf der Kommandozeile hat M. Heimpold im Mini-Howto zur Zertifikatserstellung beschrieben. http://www.heimpold.de/mhei/mini-howto-zertifikaterstellung.htm.

Komfortabler geht es mit dem Tool **XCA**, das z.B. auf der JoToSL-DVD enthalten ist (siehe Kapitel Live-DVDs).

7.2.8 Ist S/MIME-Verschlüsselung unsicher?

Nach unserer Einschätzung ist die S/MIME-Verschlüsselung wesentlich schwächer, als OpenPGP. Die Ursachen liegen nicht in einer Schwäche der verwendeten Algorithmen, sondern in der Generierung und Speicherung der privaten Schlüssel außerhalb der Hoheit des Anwenders.

Die Sicherheit asymmetrischer Kryptografie hängt entscheidend von der Vertrauenswürdikeit der privaten Schlüssel ab. Während der öffentliche Schlüssel möglichst breit zu verteilen ist, muss die Verfügungsgewalt für den privaten Schlüssel ausschließlich und vollständig(!) in der Hand des Anwenders liegen. Nur so kann gewährleistet werden, dass kein unbefugter Dritter die vertrauliche Kommunikation entschlüsseln kann.

Um die Nutzung der S/MIME-Verschlüsselung für unbedarfte Anwender zu erleichtern, wird die Erzeugung und Aufbewahrung der privaten Schlüssel häufig durch organisatorische Schwächen kompromittiert.

Erzeugen der privaten Keys

Alle Anbieter von Zertifizierungen für X.509 Zertifikate bieten eine webbasiertes Interface für die Erzeugung und Signatur der Zertifikate. In der Regel werden nach erfolgricher Überprüfung der Identität des Antragstellers zwei Varianten für die Generierung eines gültigen Zertifikates angeboten:

1. Man kann nach in einer selbst gewählten sicheren Umgebung den privaten Schlüssel und ein Certification Request (CSR) erzeugen. Der CSR enthält nur den öffentlich Schlüssel. Dieser wird im Webinterface hochgeladen und man erhält via E-Mail oder Download Link das signierte Zertifikat.

2. Man die komplette Generierung des privaten und öffentlichen Schlüssels der CA überlassen und muss darauf vertrauen, dass dieser keine Kopie des privaten Schlüssels speichert.

Aus Bequemlichkeit nutzt die absolute Mehrheit der Anwender den 2. Weg und geht damit das Risiko ein, dass die Schlüssel bereits vor der Verwendung kompromittiert werden könnte.

In einem Forschungspapier kommen die Sicherheitsforscher C. Soghoian und S. Stamm zu dem Schluss, das die US-Regierung von kooperierenden Certification Authorities die privaten Keys von X509-Zertifikaten erhalten könnte und die US-Behörden somit die Daten problemlos entschlüsseln können. Eine ähnliche Zusammenarbeit gibt es unserer Meinung nach auch zwischen Startcom-SSL und dem isrealischen Geheimdienst.

Der Deutsche Bundestag

Der Deutsche Bundestag bietet allen Abgeordneten die Möglichkeit, S/MIME für die Verschlüsselung von E-Mails zu verwenden.

Die Abgeordneten sind scheinbar nicht über diese Möglichkeit informiert. Bei der technischen Umsetzung gilt das Prinzip *Security by obscurity*, wie ein Testbericht zeigt (http://www.heise.de//tp/r4/artikel/27/27182/1.html).

Um die Abgeordneten maximal von der "komplizierten" Technik des Entschlüsseln der E-Mail zu entlasten, erfolgt die Entschlüsselung auf einem zentralen Server des Bundestages. Auf diesem zentralen Server liegen auch

die privaten Schlüssel und die Zertifikate der Abgeordneten.

Damit ist gesichert, dass auch die Sekretärinnen keine Probleme haben, wenn der Absender einer E-Mail diese verschlüsselt und damit sicherstellen wollte, dass nur der Abgordnete selbst sie lesen kann.

Hier wird eine Vertraulichkeit der Kommunikation vorgegaukelt. Gefährlich wird dieser Placebo, wenn ein Bürger auf die Sicherheit vertraut und sich gegenüber seinem Abgeordneten freimütiger äußert, als er es unverschlüsselt tun würde.

Web.de (Free-) Mail-Account

Beim Anlegen eines Mail-Accounts bei Web.de wird automatisch ein S/MIME-Zertifikat für den Nutzer generiert. Der öffentliche und der private Schlüssel liegen auf dem Server des Anbieters. Der Schlüssel ist nicht durch ein Passwort geschützt.

Dieses Feature wird von Web.de wie folgt beworben:

"Versehen Sie Ihre E-Mail mit einer digitalen Unterschrift, kann diese auf dem Weg zum Empfänger nicht verändert werden. Die digitale Verschlüsselung sorgt dafür, dass die E-Mail auf dem Weg zum Empfänger nicht gelesen werden kann."

Außerdem fordert die Website dazu auf, das Zertifikat im eigenen E-Mail Client zu importieren und für die Verschlüsselung zu nutzen.

Diese Variante von S/MIME ist ein Placebo, den man ignorieren sollte. Die Werbebotschaft entspricht nicht der Wahrheit. Gemäß geltendem Recht ist die E-Mail beim Empfänger angekommen, wenn der Empfänger Gelegenheit hatte, sie zur Kenntnis zu nehmen. Vorher kann sie jedoch auf dem Server von Web.de entschlüsselt werden (auch von stattlichen Stellen).

Projekt De-Mail

Auch das geplante Portale De-Mail für die rechtsverbindliche und sichere deutsche Alternative zur E-Mail soll X.509 Zertifikate für die Gewährleistung der vertraulichen Kommunikation nutzen. Die Anforderungen sehen eine Entschlüsselung der vertraulichen E-Mails durch Betreiber des Dienstes ausdrücklich vor. Als Grund wird die Notwendigkeit des Virescans genannt.

Außerdem wirbt das Projekt damit, den Nutzern einen "Datentresor" für vertrauliche digitale Dokumente zur Verfügung zu stellen. Das Konzept kann jedoch nur als Placebo bezeichnet werden. Sowohl die verschlüsselten Dokumente als auch die Schlüssel für den Zugriff auf die Dokumente sollen beim Anbieter des Dienstes liegen. Die Entschlüsselung der vertraulichen Daten durch Mitarbeiter ist ebenfalls ausdrücklich vorgesehen.

Das Projekt De-Mail wird in Zusammenarbeit mit dem ePA einen Key-Escrow (Hinterlegung der Schlüssel bei den Behörden) für unbedarfte An-

wender vorrantreiben. Den Anwendern wird eine Sicherheit vorgegaukelt, die durch Behörden einfach kompromittiert werden kann.

7.3 E-Mail als verschlüsseltes Dokument senden

Manchmal möchte man eine vertrauliche E-Mail an einen Kommunikationspartner schreiben, der keine Ahnung von E-Mail Verschlüsselung hat. Oder man möchte nicht, das die Schnüffelprogramme von Google, Yahoo! oder Microsoft die E-Mail lesen. Als Alternative zur E-Mail Verschlüsselung könnte man den Inhalt der Mail in verschlüsselte Dokumente packen und diese Dokumente als Anhang mit der E-Mail versenden. LibreOffice kann Dokumente mit AES256 verschlüsseln. PDF v. 1.7 verwendet ebenfalls AES256 für die Verschlüsselung, wenn ein Passwort für das Öffnen der PDF-Datei festgelegt wurde.

Das Passwort zum Öffnen der PDF-Datei teilt man dem Empfänger entweder über einen sicheren Kanal mit oder man schreibt im Text der E-Mail eine Andeutung, die nur der Empfänger interpretieren kann, bspw:

Das Passwort ist der Name der Bar, in der wir zwei Bier getrunken haben.

Man muss nicht für jede Nachricht ein neues Passwort definieren, man kann ein einmal sicher ausgetauschte Passwort natürlich auch über einen längeren Zeitraum verwenden. Das ist sicherer, als immer wieder unsichere Methoden für den Passworttausch.

7.4 Eine Bemerkung zum Abschluß

"Mache ich mich verdächtig, wenn ich meine E-Mails verschlüssel?"

Eine Frage, die häufig gestellt wird, wenn es um verschlüsselte E-Mails geht. Bisher gab es darauf folgende Antwort:

"Man sieht es einer E-Mail nicht an, ob sie verschlüsselt ist oder nicht. Wer befürchtet, dass jemand die Mail beschnüffelt und feststellen könnte, dass sie verschlüsselt ist, hat einen Grund mehr, kryptografische Verfahren zu nutzen!"

Aktuelle Ereignisse zeigen, dass diese Frage nicht mehr so einfach beantwortet werden kann. Dem promovierten Soziologen Andrej H. wurde vorgeworfen, Mitglied einer terroristischen Vereinigung nach §129a StGB zu sein. Der Haftbefehl gegen ihn wurde unter anderem mit **konspirativem Verhalten** begründet, da er seine E-Mails verschlüsselte.

Am 21.Mai 2008 wurden in Östereich die Wohnungen von Aktivisten der Tierrechtsszene durchsucht und 10 Personen festgenommen. Der Haftbefehl wurde mit Verdunklungsgefahr begründet, da die Betroffenen z.B. über verschlüsselte E-Mails kommunizierten.

Am 18.10.07 hat der Bundesgerichtshof (BGH) in seinem Urteil Az.: StB 34/07 den Haftbefehl gegen Andrej H. aufgehoben und eindeutig festgestellt, dass die Verschlüsselung von E-Mails als Tatverdacht NICHT ausreichend ist, entscheidend sei der Inhalt:

"Ohne eine Entschlüsselung der in den Nachrichten verwendeten Tarnbegriffe und ohne Kenntnis dessen, was bei den - teilweise observierten und auch abgehörten - Treffen zwischen dem Beschuldigten und L. besprochen wurde, wird hierdurch eine mitgliedschaftliche Einbindung des Beschuldigten in die 'militante gruppe' jedoch nicht hinreichend belegt."

Außerdem geben die Richter des 3. Strafsenat des BGH zu bedenken, dass Andrej H. *"ersichtlich um seine Überwachung durch die Ermittlungsbehörden wusste"*. Schon allein deshalb konnte er *"ganz allgemein Anlass sehen"*, seine Aktivitäten zu verheimlichen. Woher Andrej H. von der Überwachung wusste, steht bei http://annalist.noblogs.org.

Trotz dieses Urteils des BGH bleibt für uns ein bitterer Nachgeschmack über die Arbeit unser Ermittler und einiger Richter. Zumindest die Ermittlungsrichter sind der Argumentation der Staatsanwaltschaft gefolgt und haben dem Haftbefehl erst einmal zugestimmt.

Kapitel 8

E-Mail jenseits der Überwachung

Auch bei der Nutzung von GnuPG oder S/MIME für die Verschlüsselung von E-Mails ist es mitlesenden Dritten möglich, Absender und Empfänger zu protokollieren und anhand der erfassten Daten Kommunikationsprofile zu erstellen. Insbesondere die Vorratsdatenspeicherung und die darauf aufbauenden internationalen ETSI-Standards für Geheimdienste und Strafverfolger zeigen, dass diese nicht verschlüsselbaren Informationen für die Überwachung bedeutsam sind.

Es gibt mehrere Projekte, die einen überwachungsfreien Austausch von Nachrichten ermöglichen und somit beispielsweise für investigative Journalisten und deren Informanten den nötigen Schutz bieten und die Erstellung von Kommunikationsprofilen für E-Mails behindern. Eine universelle Lösung auf Knopfdruck gibt es nicht. Jeder muss selbst die verschiedenen Möglichkeiten vergleichen und die passende Lösung auswählen.

8.1 Anonyme E-Mail Accounts

Im Kapitel Anonymisierungsdienste gibt es Anleitungen, wie man mit JonDo & Thunderbird oder mit Tor & Thunderbird einen anonymen E-Mail Account nutzen könnte. Als E-Mail Provider kann man einen zuverlässigen Anbieter im Web nehmen. Außerdem bieten I2P und Tor spezielle Lösungen:

- Das Invisible Internet Project (I2P) bietet mit Susimail einen anonymen Mailservice inclusive SMTP- und POP3-Zugang und Gateway ins Web oder mit I2P-Bote einen serverlosen, verschlüsselten Maildienst.

- Das *Lelantos-Project* ist ein E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse http://lelantoss7bcnwbv.onion betrieben wird. *Mail2Tor* ist ein weiterer E-Mail Dienst, der von Unbekannten unter http://mail2tor2zyjdctd.onion bereitgestellt wird. Gateways ins normale Web sind bei beiden Projekten vorhanden.

Hinweis: Informationen über Langzeitkommunikation können ein Pseudonym deanonymisieren. Anhand der Freunde in der E-Mail Kommunikation sind Schlussfolgerungen auf ihre reale Identität möglich. Wenn sie einen wirklich anonymen E-Mail Account für eine bestimmte Aufgabe benötigen - z.B. für Whistleblowing - dann müssen sie einen neuen Account erstellen. Löschen sie den Account, sobald sie ihn nicht mehr brauchen.

8.2 Private Messages in Foren nutzen

Viele Diskussionsforen im Internet bieten die Möglichkeit, private Nachrichten zwischen den Mitgliedern zu verschicken. Die Nachrichten werden in der Datenbank des Forums gespeichert und nicht per E-Mail durch das Netz geschickt.

Eine böse Gruppe ganz gemeiner Terroristen könnte sich also in einem Forum anmelden, dessen Diskussionen sie überhaupt nicht interessieren. Dort tauschen sie die Nachrichten per PM (Private Message) aus und keiner bemerkt die Kommunikation. Es ist vorteilhaft, wenn das Forum komplett via HTTPS nutzbar ist und nicht beim Login HTTPS anbietet.

Die Nachrichten kann man mit OpenPGP verschlüsseln, damit der Admin des Forums nichts mitlesen kann. Die Verwendung von Anonymisierungsdiensten sichert die Anonymität.

8.3 alt.anonymous.messages

Um die Zuordnung von Absender und Empfänger zu erschweren, kann man das Usenet nutzen. In der Newsgruppe *alt.anonymous.messages* werden ständig viele Nachrichten gepostet und sie hat tausende Leser. Jeder Leser erkennt die für ihn bestimmten Nachrichten selbst. Es ist eine Art schwarzes Brett.

Es ist sinnvoll, die geposteten Nachrichten zu verschlüsseln. Dafür sollte der Empfänger einen OpenPGP-Key bereitstellen, der keine Informationen über seine Identität bietet. Normalerweise enthält ein OpnePGP-Schlüssel die E-Mail Adresse des Inhabers. Verwendet man einen solchen Schlüssel ist der Empfänger natürlich deanomynisiert.

Außerdem sollte man seine Antworten nicht direkt als Antwort auf ein Posting veröffentlichen. Da der Absender in der Regel bekannt ist (falls keine Remailer genutzt wurden) kann aus den Absendern eines zusammengehörenden Thread ein Zusammenhang der Kommunikationspartner ermittelt werden.

8.4 Mixmaster Remailer

Der Versand einer E-Mail über Remailer-Kaskaden ist mit der Versendung eines Briefes vergleichbar, der in mehreren Umschlägen steckt. Jeder Empfänger innerhalb der Kaskade öffnet einen Umschlag und sendet den darin

enthaltenen Brief ohne Hinweise auf den vorherigen Absender weiter. Der letzte Remailer der Kaskade liefert den Brief an den Empfänger aus.

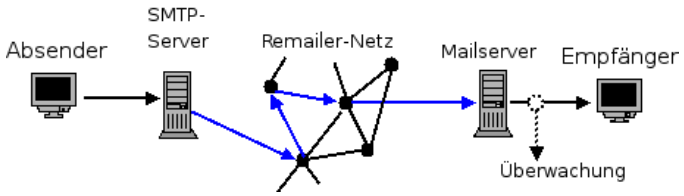


Abbildung 8.1: Konzept einer anonymen E-Mail

Technisch realisiert wird dieses Prinzip mittels asymmetrischer Verschlüsselung. Der Absender wählt aus der Liste der verfügbaren weltweit verteilten Remailer verschiedene Server aus, verschlüsselt die E-Mail mehrfach mit den öffentlichen Schlüsseln der Remailer in der Reihenfolge ihres Durchlaufes und sendet das Ergebnis an den ersten Rechner der Kaskade. Dieser entschlüsselt mit seinem geheimen Schlüssel den ersten Umschlag, entnimmt dem Ergebnis die Adresse des folgenden Rechners und sendet die jetzt (n-1)-fach verschlüsselte E-Mail an diesen Rechner. Der letzte Rechner der Kaskade liefert die E-Mail an den Empfänger aus.

Mitlesende Dritte können lediglich protokollieren, dass der Empfänger eine E-Mail unbekannter Herkunft und evtl. unbekannten Inhaltes (verschlüsselt mit OpenPGP oder S/MIME) erhalten hat. Es ist ebenfalls möglich, Beiträge für News-Groups anonym zu posten.

Um die Traffic-Analyse zu erschweren, wird die Weiterleitung jeder E-Mail innerhalb der Kaskade verzögert. Es kann somit 2...12h dauern, ehe die Mail dem Empfänger zugestellt wird! Sollte der letzte Remailer der Kette die Nachricht nicht zustellen können (z.B. aufgrund eines Schreibfehlers in der Adresse), erhält der Absender keine Fehlermeldung. Der Absender ist ja nicht bekannt.

Wichtig: Bei großen E-Mail Providern werden die anonymen E-Mails aus dem Mixmaster Netzwerk häufig als Spam einsortiert. Es ist somit nicht sichergestellt, dass der Empfänger die Mail wirklich zur Kenntnis nimmt! Oft beschweren sich Nutzer bei mir, das ihre Testmails an den eigenen Account nicht ankommen, weil sie auch nicht in den Spam-Ordner schauen.

Wichtig: Da die E-Mail keine Angaben über den Absender enthält, funktioniert der *Antworten-Button* der Clients auf der Empfängerseite nicht! Die Antwort-Mail geht dann an den letzten Remailer der Kette, der sie in die Tonne wirft. Der Text der anonymen E-Mail sollte einen entsprechenden Hinweis enthalten!

Software zur Versendung anonymer E-Mails via Mixmaster:

- Für Windows gibt es *Quicksilver* https://quicksilvermail.net

- Für Linux und BSD gibt es *mixmaster*. Das Paket ist in allen Linux Distributionen enthalten und kann mit dem bevorzugten Tool zur Paketverwaltung installiert werden.

Mixmaster installieren (Linux, BSD)

Mixmaster ist ein Kommandozeilen Tool, welches die Nachrichten mehrfach verschlüsselt an das Remailer Netzwerk übergibt. Für Debian, Ubuntu und Mint gibt es fertige Pakete in den Repositories. Die Installation folgt dem üblichen Schema:

```
> sudo apt install mixmaster
```

Die Sourcen von Mixmaster stehen unter http://mixmaster.sourceforge.net zum Download bereit. Für die Übersetzung werden die Entwicklerpakete folgender Komponenten benötigt, welche von nahezu allen Distributionen bereitgestellt werden:

- vi Editor
- ncurses Bibliothek
- OpenSSL Bibliothek
- PCRE Bibliothek
- zlib Bibliothek
- OpenPGP Programm (z.B. GnuPG)

Nach dem Download ist das Archiv zu entpacken und in das neu angelegte Verzeichnis zu wechseln. Hier ist das Kommando *./Install* einzugeben.

Die Installationsroutine stellt einige kurze Fragen und bietet sinnvolle Vorgaben. Als Installationsverzeichnis ist es sinnvoll *$HOME/.Mix* zu übernehmen. Die Frage *Do you want to set up a remailer?* ist mit ENTER zu verneinen.

Die Meldung *Client installation complete.* zeigt den erfolgreichen Abschluss der Installation an.

Mixmaster konfigurieren

Die Konfiguration von Mixmaster erfolgt in der Datei *$HOME/.Mix/mix.cfg*. Linux wird an dieser Stelle seinem Ruf als Volltext Adventure gerecht.

1. Für die Versendung an den ersten Remailer der Kaskade wird ein Absender und eine Absenderadresse benötigt. Der erste Remailer der Kaskade entfernt diese Angaben, sie werden nicht(!) an den Empfänger übermittelt. Es sind folgende Zeilen in der Konfiguration hinzuzufügen:

   ```
   NAME <absendername>
   ADDRESS <absender_email_adresse>
   ```

2. Außerdem ist die Versandart der Mail an den ersten Remailer der Kaskade zu konfigurieren. In der Regel wird man den SMTP-Server eines E-Mail Providers für die Versendung nutzen. Dafür muss man den Mail-Server und die Login Credentials konfigurieren. Die Daten findet man auf der Webseite des Mailproviders:

```
SMTPRELAY mail.server.tld
SMTPUSERNAME <smtp_nutzer_name>
SMTPPASSWORD <Passwort>
```

3. In der Konfiguration sind die Schlüsselringe für OpenPGP-Verschlüsselung anzugegeben:

```
PGPPUBRING /home/<user>/.gnupg/pubring.gpg
PGPSECRING /home/<user>/.gnupg/secring.gpg
```

4. Außerdem sind die Speicherorte für die Statusdateien des Mixmaster Netzwerkes zu konfigurieren. Am einfachsten speichert man die Dateien im Verzeichnis *$HOME/.Mix*

```
PGPREMPUBASC /home/<user>/.Mix/pubring.asc
PUBRING /home/<user>/.Mix/pubring.mix
TYPE1LIST /home/<user>/.Mix/rlist.txt
TYPE2REL /home/<user>/.Mix/mlist.txt
TYPE2LIST /home/<user>/.Mix/type2.list
```

5. Optional kann man mit CHAIN die Länge der Remailer Kasakde konfigurieren und mit NUMCOPIES mehrere Kopien der E-Mail versenden, um die Wahrscheinlichkeit der Zustellung bei Problemen mit einem Remailer zu verbessern. Um zwei Kopien der E-Mail über unterschiedliche Wege mit 5 statt 3 Remailern pro Kaskade zu versenden, sind folgende Optionen zu konfigurieren:

```
CHAIN *,*,*,*,*
NUMCOPIES 2
```

   Werden mehrere Kopien versendet, da schickt der letzte Remailer der Kaskade nur eine E-Mail an den Empfänger und löscht alle weiteren Kopien.

Nachdem man die Konfiguration gespeichert hat, muss man die Liste der verfügbaren Pinger herunterladen. Die sogenannten Pinger stellen die Informationen über die verfügbaren Remailer bereit. Die Liste der Pinger wird mit mit folgendem Kommando heruntergeladen:

```
> mixmaster --update-pinger-list
```

Anonyme E-Mails mit Mixmaster versenden

Man kann Mixmaster auf der Kommandozeile im Terminal starten und mit dem rudimentären Menü aus dem letzten Jahrhundert ein E-Mail schreiben und anonym versenden. Standardmäßig nutzt Mixmaster den Editor *vi*, was ein Krampf ist. Besser ist es, vor dem Start einen brauchbaren Texteditor wie *gedit, kwrite* oder *mousepad* auszuwählen:

```
> export EDITOR gedit
> mixmaster
```

Eine zweite Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um die E-Mail auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To:
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset=''utf-8''
Content-Transfer-Encoding: 8bit

Hallo alle miteinander,
hier beginnt der Inhalt
```

In den ersten beiden Zeilen ist die E-Mail-Adresse des Empfängers und der Betreff der Nachricht einzutragen. Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Nachdem die Nachricht geschrieben wurde, ist die Datei unter einem neuen Namen als TXT-Datei zu speichern, beispielsweise unter *$HOME/anon-email.eml*.

Diese E-Mail kann mit den folgenden Befehlszeilen versendet werden, welche für häufige Nutzung auch als Shell-Script gespeichert werden können:

```
> mixmaster --update-stats=noreply
> mixmaster -m ~/anon-email.eml
> mixmaster -S
> shred -u ~/anon-email.eml}
```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind. Unter Debian GNU/Linux ist *mixmaster-update* zu nutzen.

Die zweite Befehlszeile übernimmt die Nachricht, wählt die Remailer-Kette aus und legt eine vorbereitete E-Mail im Spool-Verzeichnis ab. Der dritte Aufruf von Mixmaster versendet alle Mails aus dem Spool-Verzeichnis und der letzte Befehl beseitigt die Datei, indem sie zuerst mit Nullen überschrieben und anschließend gelöscht wird.

Soll die E-Mail an der Empfänger OpenPGP verschlüsselt ausgeliefert werden, ist die zweite Befehlszeile zusätzlich um die Option *–encrypt* zu erweitern.

Im Prinzip ist es auch möglich, Attachements an eine anonyme E-Mail zu hängen. Viele Remailer entfernen diese jedoch. Einige Remailer lassen Attachements bis zu 100KB passieren. Ich bin der Meinung, man kann auf Anhänge verzichten und werde hier nicht weiter darauf eingehen.

Anonymes Usenet Posting mit Mixmaster versenden

Ein anonymes Usenet-Posting wird als E-Mail an ein Mail2News Gateway geschickt. Diese E-Mail wird durch die Ramailer-Kaskade anonymisiert. Das Gateway wandelt die anonyme E-Mail in ein News-Posting um und schickt es an die Newsgroups.

- mail2news (at) bananasplit.info
- mail2news (at) dizum.com
- mail2news (at) reece.net.au
- mail2news (at) m2n.mixmin.net

Wie beim Schreiben einer anonymen E-Mail gibt es zwei Möglichkeiten, um ein anonymes Usenet-Posting zu schreiben. Man kann mixmaster auf der Kommandozeile starten:

```
> export EDITOR gedit
> mixmaster
```

Nach der Aktualisierung der verfügbaren Remailer mit [u] kann man ein Usenet-Posting verfassen mit [p] und anschließend mit [s] versenden.

Eine zweite Möglichkeit nutzt einen beliebigen **Texteditor** oder besser eine komplette Textverarbeitung mit Rechtschreibprüfung und Vorlagenverwaltung, um das Posting auf Basis der folgenden Vorlage zu schreiben, als TXT-Datei zu speichern und diese mit Mixmaster anonym zu versenden.

```
To: mail2news@newsanon.org, mail2news@dizum.org
Newsgroups:
X-No-Archive: Yes
Subject:
Mime-Version: 1.0
Content-Type: text/plain; charset=‘‘utf-8’’;
Content-Transfer-Encoding: 8bit

Ich möchte folgendes veröffnetlichen: blabla
```

Zwischen dem Header und dem eigentlichen Inhalt ist eine Leerzeile frei zu lassen.

Nachdem die Nachricht geschrieben wurde, ist die Datei im TXT-Format unter einem neuen Namen zu speichern, beispielsweise unter *$HOME/anon-news.eml*. Diese Datei kann mit den folgenden Befehlszeilen an die Newsgroups gesendet werden:

```
> mixmaster --update-stats=noreply
> mixmaster -m ~/anon-news.eml
> mixmaster -S
> shred -u ~/anon-news.eml
```

Der erste Befehl aktualisiert die Remailer-Statistiken und kann entfallen, wenn diese nicht älter als 24h sind.

Mixmaster mit Tor Onion Router verwenden

Man kann Mixmaster mit dem Anonymisierungsdienst Tor kombinieren. Ein Beobachter kann damit nicht erkennen, dass eine anonyme E-Mail via Mixmaster versendet wurde.

Dafür benötigt man neben Tor Onion Router und dem Tor-GUI *Vidalia* entweder das Tool *torify* oder *torsocks*. Der Tor Daemon muss am Port 9050 lauschen, damit diese beiden Tools korrekt funktionieren.

Es gibt zwei Tor Hidden Services, die als SMTPRELAY genutzt werden können. Einer dieser beiden Tor Hidden Services sollte in der Konfigurationsdatei *mix.cfg* als SMTP-Server eingetragen werden. Für diese beiden SMTP-Server muss man keine Login Credentials angeben. Als Beispiel eine komplette, funktionsfähige Konfigurationsdatei, in der man nur <USERNAME> durch den eigenen Namen ersetzen muss:

```
NAME Anonymous
ADDRESS ano@nymous.net

SMTPRELAY gbhpq7eihle4btsn.onion

CHAIN *,*,*
NUMCOPIES 2

PGPPUBRING /home/<USERNAME>/.gnupg/pubring.gpg
PGPSECRING /home/<USERNAME>/.gnupg/secring.gpg

PGPREMPUBASC /home/<USERNAME>/.Mix/pubring.asc
PUBRING /home/<USERNAME>/.Mix/pubring.mix
TYPE1LIST /home/<USERNAME>/.Mix/rlist.txt
TYPE2REL /home/<USERNAME>/.Mix/mlist.txt
TYPE2LIST /home/<USERNAME>/.Mix/type2.list
```

Alternativ kann man den Tor Hidden Service vom Remailer *frell* nutzen. Dieser SMTP-Server nimmt nur E-Mails für *frell* an. Folgende Zeilen sind in dem Beispiel zu ersetzen:

```
SMTPRELAY zvrqjaxpgxglgjrz.onion
CHAIN frell,*,*
```

Nach Anpassung der Konfiguration startet man Tor und danach Mixmaster unter Kontrolle von *torify* oder *torsocks*. Der bevorzugte Editor ist mit *export* zu setzen, damit man sich nicht bei der Bedienung des Standardeditors vi Gehirnzellen und Finger verrenkt:

```
> export EDITOR gedit
> torify mixmaster
```

Kapitel 9

Instant Messaging

Instant Messaging und Chat können für sogenannte synchrone Kommunikation genutzt werden. Wie beim Telefonieren müssen die Kommunikationspartner gleichzeitig online sein und direkt miteinander in Kontakt treten. Das hat den Vorteil, dass die Inhalte nicht auf Servern zwischengespeichert werden müssen und teilweise auch direkt zwischen den Beteiligten ausgetauscht werden. Gegenüber E-Mail bietet Instant Messaging den Vorteil, dass die Metadaten der Kommunikation nicht so einfach ermittelt werden können.

Die Kontaktadressen werden wie bei E-Mails folgermaßen gebildet:

```
<username>@server.tld
```

Wenn man seine Adresse weitergibt oder veröffentlicht, muss man zusätzlich angeben, um welchen Dienst es sich handelt (XMPP, SILC...), um Missverständnisse zu vermeiden.

9.1 Jabber (XMPP)

Jabber (XMPP) ist ein offenes Protokoll, das eine förderalistische Infrastruktur ermöglicht. Wie bei E-Mail kann man einen Anbieter wählen, der am besten die eigenen Präverenzen erfüllt und trotzdem mit allen anderen kommunizieren. Wenn der Anbieter seine Policies ändert, kann man zu einem besseren Anbieter wechseln ohne das Netzwerk der Kontakte zu verlieren, man muss nur die eigene, neue Kontaktadresse verteilen. Das unterscheidet Jabber/XMPP wesentlich von neumodischen Messaging Diensten wie WhatsApp o.ä.

Ende-zu-Ende Verschlüsselung

Ende-2-Ende-Verschlüsselung ist für Instant Messaging mindestens so wichtig, wie für E-Mail. Die Auswertung von 160.000 Überwachungsberichten aus dem Snowden-Fundus zeigt, dass die Geheimdienste diese Kommunikation massiv überwachen.

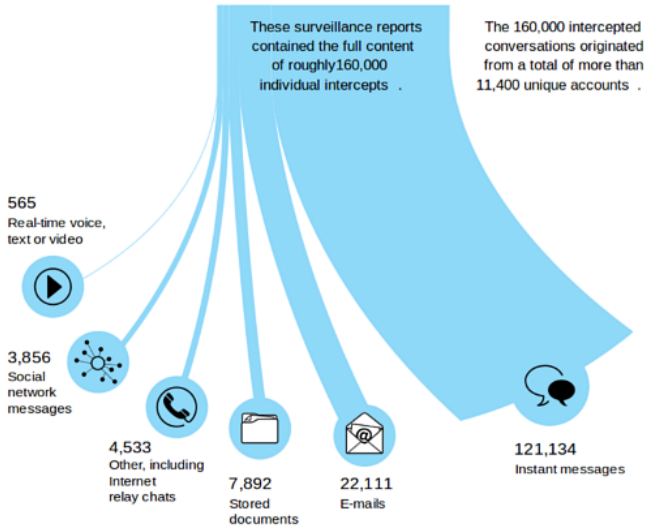


Abbildung 9.1: Auswertung von 160.000 Überwachungsberichten

Jabber wurde primär für die direkte Kommunikation zwischen zwei Teilnehmern entwickelt. Für den Chat zwischen zwei Partnern gibt es folgende Verfahren zur Ende-zu-Ende Verschlüsselung der Kommunikation:

OTR (Off-the-Record) wurde von den Cypherpunks mit dem Ziel entwickelt, möglichst einfach einsetzbar zu sein. Eine OTR-verschlüsselte Verbindung wird automatisch aufgebaut, wenn beide Jabber-Clients dieses Feature unterstützen.

Allerdings muss die Vertrauenswürdigkeit der Verschlüsselung von den Teilnehmern verifiziert werden. Ohne diese Prüfung könnte sich ein Lauscher als man-in-the-middle einschleichen. Die Software für diesen Angriff gibt es auch als Open Source, z.B. *mod_otr* für ejabberd. Für die Verifikation der Schlüssel bietet OTR drei Möglichkeiten:

- Vergleich der Fingerprints der Schlüssel.
- Verifizierung mit einem gemeinsamen Passwort.
- Verifizierung durch Frage und Antwort.

Beide Kommunikationspartner müssen die Fingerprints der Schlüssel bzw. das gemeinsame Passwort oder die Frage/Antwort über einen unabhängigen, sicheren Kanal austauschen (zum Beispiel bei einem persönlichen Treffen), bevor sie die OTR-Verschlüsselung verfizieren können.

OpenPGP wurde bereits bei der Verschlüsselung von E-Mail behandelt. Die Erstellung und Austausch der Schlüssel ist etwas komplizierter als bei OTR. Die Vertrauenswürdigkeit der Verschlüsselung muss aber nicht

extra verifiziert werden, da sie durch das Vertrauen in die OpenPGP-Schlüssel gegeben ist.

OpenPGP für Jabber/XMPP gibt es in zwei Standards. Die meisten Jabber Clients implementieren XEP-0027, der inzwischen für obsolet erklärt wurde, da er einige Sicherheitslücken enthält. Der neuer XEP-0373 ist bisher noch als experimentell gekennzeichnet und wird nur von sehr wenigen Jabber Clients unterstützt.

OMEMO (OMEMO Multi-End Message and Object Encryption) ist eine relativ neue Ende-zu-Ende Verschlüsselung für Jabber/XMPP. Sie basiert auf Axolotl Ratchet, das von WhisperSystems für TextSecure entwickelt wurde. Sie bietet wie OTR einen automatischen Schlüsseltausch, Forward Secrecy und Deniability. Zusätzlich bietet OMEMO verschlüsselte Offline-Messages und verschlüsselten Dateitransfer via HTTPUpload für Bilder, was mit OTR nicht möglich ist. Außerdem kann OMEMO in der Regel auch dann problemlos genutzt werden, wenn man mit mehreren Geräten gleichzeitig online ist.

Bisher gibt es OMEMO nur für die Smartphone Clients *Conversations* (Android) und *ChatSecure* (iOS) sowie für den Desktop Client *Gajim*. Um OMEMO für die Ende-zu-Ende Verschlüsselung nutzen zu können, muss der Server die XMPP-Erweiterungen XEP-0163 und XEP-0280 unterstützen.

Für den XMPP Client Pidgin gibt es auch ein OMEMO Plug-in. Das Plug-in muss man derzeit noch selbst compilieren, es steht noch nicht als Binary zur Verfügung. Dieses Plug-in vergrößert das Chaos bei der OMEMO-Verschlüsselung weiter. Da Pidgin keine Carbons kennt und kein MAM können Offline Messages im Gegensatz zu anderen OMEMO Implementierungen nicht verschlüsselt werden und die Nutzung mehrerer Gerät gleichzeitig wird auch nicht unterstützt. Damit bietet OMEMO für Pidgin kaum Vorteile gegenüber der ausgereifteren OTR-Verschlüsselung.

Ende-zu-Ende Verschlüsselung für XMPP Erweiterungen

Jabber/XMPP bietet neben der direkten Kommunikation zwischen zwei Partnern viele Erweiterungen. Es gibt Gruppenchats, Jingle Dateitransfer oder Audio- und Video-Chats. Diese erweiterten Funktionen sind in der Regeln nicht Ende-zu-Ende verschlüsselt.

OMEMO versucht diese Lücke zu schließen und bietet folgende Features:

- Ende-zu-Ende Verschlüsselung funktioniert für private(!) Gruppenchats, in denen alle Teilnehmer sich gegenseitig in die Kontaktliste aufgenommen haben und die OMEMO-Schlüssel durch einen direkten Chat untereinander ausgetauscht haben.
- Verschlüsselter Austausch von Bildern funktioniert manchmal via HTTPUpload. Dafür funktioniert der Tausch anderer Dateiformate nicht mehr

mit Gajim via HTTPUpload oder nur eingeschränkt, da der Empfänger nur verschlüsselten Müll via Download Link enthält.

- D. Gultsch hat mit OMEMO Encrypted Jingle File Transfer einen Vorschlag eingereicht, wie man diesen Dateitransfer mit OMEMO verschlüsseln könnte.

Im Moment ist die Situation mit den erweiterten XMPP-Features und OMEMO etwas chaotisch und unübersichtlich. Man kann sich (noch) nicht darauf verlassen, dass es mit jedem Kommunikationspartner problemlos funktioniert.

Jabber Clients

Um Jabber/XMPP zu nutzen installiert man einen Instant Messaging Client (z.B *Gajim* mit den evtl. nötigen Plug-ins, erstellt einen (meist) kostenlosen Account auf einem Jabber-Server, aktiviert die OTR- oder OpenPGP-Verschlüsselung und kann loslegen. (Vorbereitung: 3-5min)

Für den Desktop PC gibt es mit Plugins aufmotzbare, Feature-reiche Jabber Clients wie z.B. *Gajim, Pidgin* und andere, bei denen der Spaßfaktor im Vordergrund steht und Sicherheit der Kommunikation nur eine untergeordnete Rolle spielt. Wer in erster Linie Spaß an der Kommunikation haben möchte, kann als Linux User den bevorzugten Jabber Client mit der Paketverwaltung installieren und aktuell halten. Windows und MacOS Nutzer finden Installationspakete auf den Webseiten der Projekte.

Wir haben uns Pidgin und Gajim unter Linux angeschaut und ...

- Wenn man Pidgin für Debian verwenden will, dann wird zusätzlich das Paket *gstreamer-plugins-bad* installiert, damit man sofort via Video und Audio chatten kann. Die Codecs in diesem Paket enthalten viele Bugs, deshalb heißen sie BAD. Die Installation dieser Codecs ist ein Sicherheitsrisiko! Wenn diese Codecs installiert wurden, kann unter Umständen der Aufruf einer bösartigen Webseite im Browser Google Chrome ausreichen, um den Computer zu kompromittieren.[1]

  Wenn man das Paket *gstreamer-plugins-bad* deinstalliert, dann ist auch Pidgin wieder weg. Debianer müssten sich einen sicheren Pidgin selbst bauen.

- Die Crypto-Plugins für die OTR- und OMEMO-Verschlüsselung für Gajim sind EXPERIMENTELL und man muss sie mit dem Plugin Installer installieren. Seit 2013 gibt es einen Bug im Gajim Plugin Installer, die SSL-Zertifikate für die Verbindung zum Download Server wurden nicht verifiziert (der Bug wurde Dez. 2016 gefixt, aber Zertifikatspinning fehlt weiterhin). Außerdem gibt es keine Verifikation für die Integrität der heruntergeladenen Plugin Archive (Bug 79 von 2013).

[1] http://www.golem.de/news/chrome-gstreamer-windows-10-sicherer-als-linux-desktops-1611-124535.html

Wenn ein böser Bube die Ende-zu-Ende Verschlüsselung eines Gajim Nutzers kompromittieren möchte (z.B. ein Geheimdienst wie der BND mit einem Budget von 150 Mio. Euro zum Knacken von Messengern Diensten), dann könnte er einen eigenen Server aufsetzen, das Opfer via DNS-Manipulation auf den Server leiten und ein modifiziertes OTR- oder OMEMO-Plugin mit Masterschlüssel für die Dienste zum Download anbieten. Die Gajim E2E-Crypto ist also nicht für hohe Sicherheitsanforderungen geeignet.

- Pidgin und Gajim haben eine vorbereitete Proxy Konfiguration für Tor Onion Router und suggerieren damit, dass es möglich wäre, Tor mit diesen beiden Jabber Clients zu nutzen. Kann man machen - aufgrund von Bugs sollte man aber NICHT erwarten, dass man anonym bleiben kann.

Daneben gibt es für den Desktop PC die auf Sicherheit optimierten Jabber Clients *TorMessenger* oder *CoyIM* (beide noch im Beta Stadium), die aus Sicherheitsgründen nur Plain XMPP mit OTR-Verschlüsselung können und keine Erweiterungen wie Gruppenchats oder Dateitransfer unterstützen.

Nur diese beiden Clients sind auch für die Nutzung via Tor Onion Router geeignet, wenn man wirklich anonym bleiben will. *TorMessenger* oder *CoyIM* sollten immer(!) in Kombination mit Tor Hidden Jabber Servern genutzt werden, deshalb werden sie im Kapitel *Anonymes Instant Messaging mit Tor* vorgestellt. Beim TorMessenger ist der Grund offensichtlich, bei CoyIM liegt es an der grottenschlechten TLS Package von Golang.

- Die TLS Package von Golang kann keine aktuellen AES-GCM Cipher verwenden sondern nur AES-CBC-SHA Ciphersuiten, die außerdem noch via Lucky13 Attack (2013 publiziert) angreifbar sind, und RC4 Cipher, die nach den Empfehlungen der IETF (RFC 7465) und des BSI (TR-02102-2) nicht mehr genutzt werden sollten. Da den Entwicklern der TLS Package von Golang die Probleme mit Lucky13 bekannt sind, werden RC4 Cipher bevorzugt. Diese Schwäche von CoyIM kann man kompensieren, wenn Tor Onion Router die Transportverschlüsselung zum Hidden Jabber Server sicherstellt.

Auch auf dem Smartphone kann man Jabber/XMPP als Messenger nutzen. Für Android empfehlen wir die App *Conversations*, die OTR, OpenPGP und OMEMO beherrscht. Für iPhones gibt es *ChatSecure*. Ein neues Projekt ist *Zom*, das als Nachfolger von ChatSecure für Android und iPhone ein modernes GUI mit dem Unterbau von Conversations verbindet.

Jabber Server

Um Jabber/XMPP für die Kommunikation nutzen zu können, muss man einen Account auf einem Jabber Server anlegen. Es gibt eine große Auswahl von Servern und es fällt schwer, eine Auswahl zu treffen. Folgende Kriterien kann man beachten:

- Um die moderne OMEMO Verschlüsselung verwenden zu können, muss der Server die notwendigen Erweiterungen XEP-0163 und XEP-0280 unterstützen. Ob der bevorzugte Server diese Extensions unterstützt, kann

man entweder selbst mit dem Java Programm ComplianceTester for XMPP[2] prüfen oder auf der Webseite von D. Gultsch[3] nachschauen, wo man die Testergebnisse für einige Server findet.

- Wenn man Jabber/XMPP auch auf dem Android Smartphone verwenden möchte, dann kann man mit Server Push Notifications (XEP-0357) den Akku schonen.

- Der Server sollte eine SSL/TLS Verschlüsselung nach dem Stand der Technik bieten. Das kann man beim IM Observatory[4] prüfen oder mit dem CryptCheck, indem man folgende URL aufruft: *https://tls.imirhil.fr/xmpp/<domain.tld>*

- Die SSL/TLS Transportverschlüsselung bietet nur hinreichende Sicherheit und schützt gegen passive Lauscher am Draht. Ein potenter Angreifer, der gültige X509 Zertifikate faken kann (z.B. Geheimdienste), könnte mit einem gezielten Angriff als man-in-the-middle die SSL/TLS Verschlüsselung aushebeln. Tor Hidden Services bieten hohe Sicherheit und schützen auch gegen diese Angriffe. Wer hohe Sicherheit benötigt, sollte ein Jabber Server mit Tor Hidden Service nutzen (siehe: Tor Onionland). Hinweise zur Konfiguration der Jabber Clients gibt es im Kapitel Anonymisierungsdienste.

- Für langfristige Nutzung könnte man darüber nachdenken, ob es ein plausibles Konzept zur Finanzierung der Server gibt oder ob man mit dem Risiko leben möchte, dass der Betrieb kurzfristig eingestellt werden könnte weil der Admin keine Lust mehr hat.

Ein kleine Liste der von uns empfohlenen XMPP-Servern:

Anbieter	OMEMO	Tor Hidden Service	Bemerkung
conversations.im	ja		kostenpflichtig
jabber.calyxinstitute.org	nein	ijeeynrc6x2uy5ob.onion	erzwingt OTR
draugr.de	ja	jfel5icoxf3nmftl.onion	Spenden-finanziert
mailbox.org	ja	kqiafglit242fygz.onion	nur für Kunden
jabber.cat	ja	sybzodlxacch7st7.onion	von der Jabber-Katze
trashserver.net	ja	m4c722bvc2r7brnn.onion	Spenden-finanziert

Die Aufzählung ist unvollständig, als kleine Anregung gedacht. Umfangreichere Listen gibt es beim IM Observatory[5] (mit einer Bewertung der SSL-Verschlüsselung), bei jabberes.org oder bei xmpp.org.

Bei spendenfinanzierten Servern kann man für private Accounts 10-15 Euro pro Jahr investieren, um den Betreiber zu einem langfristigen und stabilen Betrieb des Dienstes zu motivieren.

[2] https://github.com/iNPUTmice/ComplianceTester
[3] https://gultsch.de/compliance_ranked.html
[4] https://xmpp.net
[5] https://xmpp.net/directory.php

9.2 Jabber/XMPP Client Gajim

Gajim ist ein Jabber/XMPP Client, der neben OpenPGP- und OTR-Verschlüsselung auch die neue OMEMO-Verschlüsselung beherrscht (noch unvollständig und experimentell). OTR und OMEMO werden dabei über Plugins bereitsgestellt, OpenPGP ist fest eingebaut.

Installation

Windows Nutzer laden die Installationsdatei von der Download Webseite herunter und starten die EXE-Datei als Administrator.

Debian 8 (jessie) Nutzer können Gajim zusammen mit dem OMEMO-Plugin aus den Backports zu installieren. Als erstes fügt man das Backports-Repository hinzu:

```
> sudo add-apt-repository 'deb http://ftp.debian.org/debian jessie-backports main
> sudo apt update
```

Danach installiert man Gajim und das OMEMO-Plugin aus den Backports und die anderen benötigten Pakete aus dem Standard Repository:

```
> sudo apt -t jessie-backports install gajim gajim-omemo
> sudo apt install python-potr python-openssl kwalletcli
> sudo apt install aspell-de libgtkspell0
```

Das Paket *python-potr* wird für das OTR-Plugin benötigt. *kwalletcli* ist optional und ermöglicht es, die Zugangsdaten verschlüsselt in der Passwortverwaltung KWallet zu speichern. aspell und die sprachspezifischen Wörterbücher werden für die Rechtschreibprüfung verwendet. Anschließend startet man Gajim und installiert das Plugin für die OTR-Verschlüsselung mit der Plugin-Verwaltung von Gajim.

Ubuntu 16.04+ Nutzen können folgende Pakete zu installieren:

```
> sudo apt install gajim python-axolotl python-protobuf python-potr
> sudo apt install kwalletcli aspell-de libgtkspell0 python-openssl
```

Die Pakete *python-axolotl* und *python-protobuf* werden für das OMEMO-Plugin benötigt. Anschließend startet man Gajim und installiert die Plugins für die OMEMO- und OTR-Verschlüsselung mit der Plugin-Verwaltung von Gajim.

Mit Gajim könnte man auch per Audio- oder Video-Chats chatten. Dafür müsste man unter Linux die Pakete *python-farstream* und *gstreamer-plugins-bad* installieren. Das sollte man nicht tun! Die *gstreamer-plugins-bad* heißen bad, weil sie BAD sind und viele Bugs enthalten. Die Installation dieser Codecs ist ein Sicherheitsrisiko. Wenn diese Codecs installiert wurden, kann unter Umständen der Aufruf einer bösartigen Webseite im Browser Google Chrome ausreichen, um den Computer zu kompromittieren.[6]

[6] http://www.golem.de/news/chrome-gstreamer-windows-10-sicherer-als-linux-desktops-1611-124535.html

Installation der Plugins

Nach der Installation startet man Gajim, überspringt den Assistenten zur Einrichtung eines Account und öffnet die Plugin-Verwaltung unter *Ändern - Plugins*. Auf dem Reiter der verfügbaren Plugins wählt man das OTR-Plugin und das OMEMO-Plugin sowie HTTPUpload und klickt auf den Button *Install/Upgrade*.

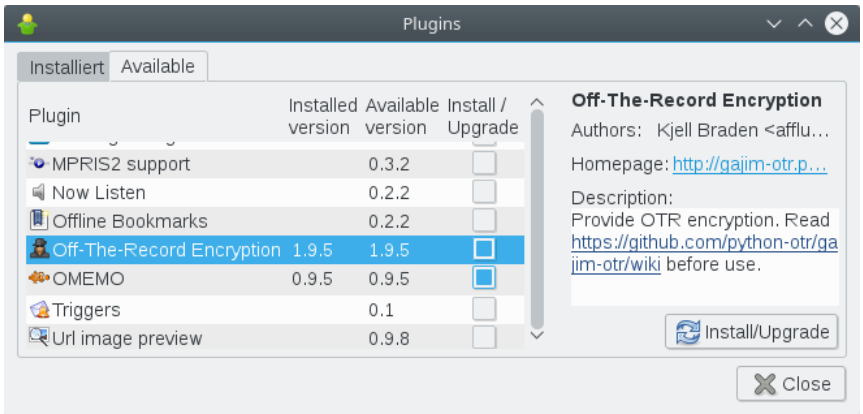


Abbildung 9.2: Gajim: Plugins installieren

Nach der Installation muss man die Plugins noch aktivieren. Dafür wechselt man zum Reiter Ïnstalliertünd aktiviert die frisch installierten Plugins.

Konfiguration von Gajim

Bevor man einen Account erstellt, kann man noch einige Anpassungen der Konfiguration vornehmen. Dazu öffnet man den Konfigurationsdialog (Menüpunkt: *Ändern - Preferences*) und klickt sich einmal durch die Einstellungen. Auf dem Reiter *Erweitert* kann man die bevorzugten Programme konfigureren und Einstellungen zur Privatspäre vornehmen. Wichtig ist beispielsweise, die Aufzeichnung von verschlüsselten Chats zu deaktivieren. Die Protokollierung verschlüsselter Sitzungen ist ein Security Bug, der C. Mannings zum Verhängnis wurde.

Wenn man den *Erweiterten Konfigurationseditor* öffnet, kann man die Rechtschreibprüfung aktivieren. Dazu trägt man die gewünschte Sprache ein (Deutsch: *de_DE*) und aktiviert die Rechtschreibprüfung, wie es im Screenshot zu sehen ist. Gajim verwendet das Programm *aspell* für die Rechtschreibprüfung. Die Wörterbücher für die gewünschte Sprache und die *libgtkspell0* müssen unter Linux ebenfalls installiert sein.

Account erstellen

Um einen Jabber/XMPP Account einzurichten öffnet man die Accountverwaltung (Menüpunkt: *Ändern - Konten*) und klickt auf den Button *Hinzufügen*. Es

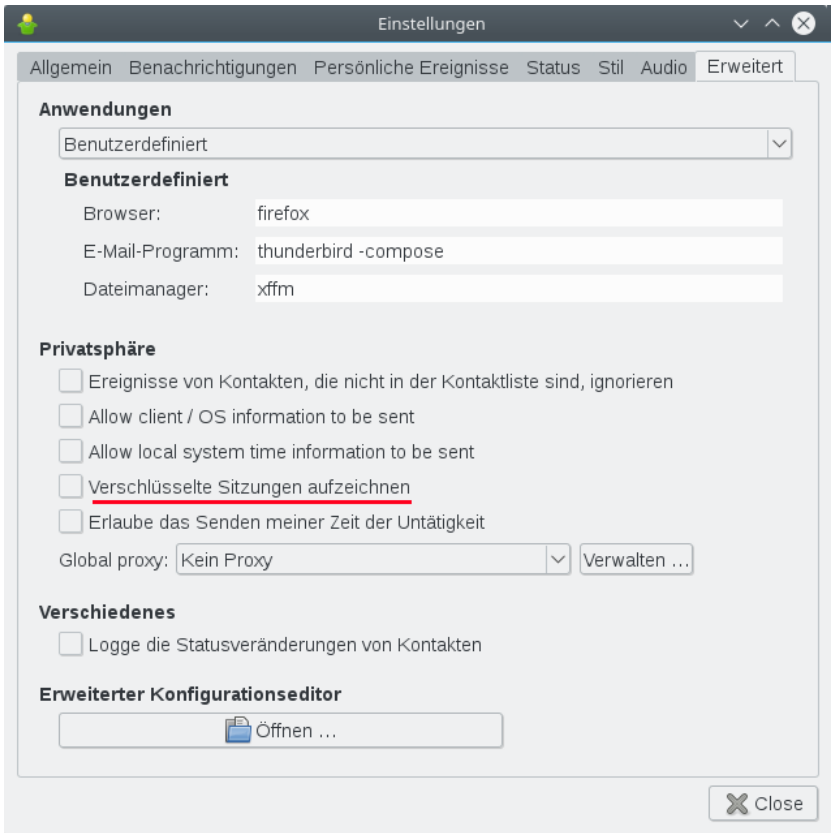


Abbildung 9.3: Gajim: Konfiguration

öffnet sich der Assistent zur Konfiguration neuer Konten und man hat zwei Möglichkeiten:

1. Wenn man bereits einen Account hat, die ist Konfiguration einfach. Man uss nur den Namen des Account und die Domain eingeben. Das Passwort muss man nicht speichern, es wird dann beim Herstellen der Verbindung abgefragt.

2. Wenn man einen neuen Account auf einem Jabber Server erstellen möchte, wählt man zuerst den Server. Das Drop-Down Menü enthält eine Liste von Jabber Servern.

   Danach wählt man den Namen und das Passwort für den neuen Account. An dieser Stelle muss man das Passwort eingeben, weil es für die Einrichtung des Account auf dem Server benötigt wird. Einige Server verlangen die Lösung für ein Captcha, um Robots die Anmeldung zu erschwerden.

Account konfigurieren

In den erweiterten Einstellungen des Account kann man nach dem Erstellen des Account noch einige Kleinigkeiten anpassen. Gajim möchte z.B. wieder alle Unterhaltungen protokollieren (das betrifft auch verschlüsselte Konversationen). Außerdem kann man das Verfolgen von Konversationen auf anderen Geräten deaktivieren, da es nicht mit der OTR-Verschlüsselung kompatibel ist, man sieht dann nur unlesbaren OTR-Kauderwelsch. Mit OpenPGP und OMEMO gibt es keine Probleme.

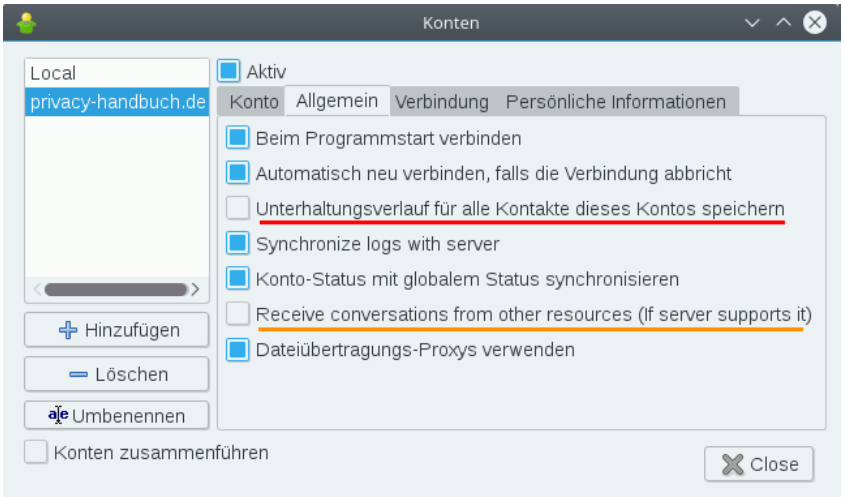


Abbildung 9.4: Gajim: Account konfigurieren

In dem grafischen Einstellungsdialog kann man nur den Dateitransfer Proxy aktivieren. Man kann aber nicht den gewünschten Server konfigurieren. Standardmäßig nutzt Gajim die Server *proxy.eu.jabber.org*, *proxy.jabber.ru* und *proxy.jabbim.cz*. Wenn man den Dateitransfer Proxy des bevorzugten Jabber Servers nutzen möchte, weil man diesem Provider mehr vertraut, dann muss man den Proxy im *Erweiterten Konfigurationseditor* anpassen. Den Konfigurationseditor findet man im Einstellungsdialog (*Ändern - Preferences*) auf dem Reiter *Erweitert*. Dort kann man nach file_transfer_proxies für den Account suchen und den Wert editieren.

Außerdem kann man in dem Konfigurationseditor die Einstellungen für die SSL/TLS- Verschlüsselung anpassen. Standardmäßig verwendet Gajim TLS v1.0+ und eine schwache Cipherliste HIGH:!aNULL:RC4-SHA, die nicht mehr mit den aktuellen Empfehlungen der IETF RFC 7525 kompatibel ist. Für jeden Account kann man folgende Werte anpassen:

```
tls_version = 1.2
cipher_list = ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384
```

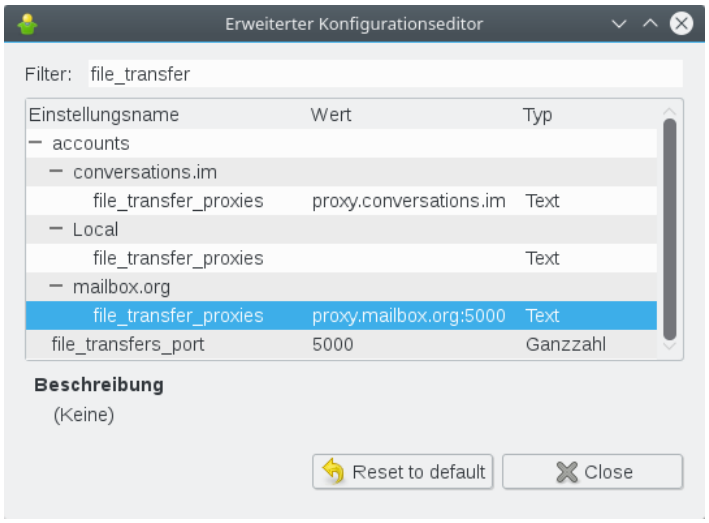


Abbildung 9.5: Gajim: Dateitransfer Proxy eintragen

Kapitel 10

Verschlüsselt telefonieren

Der bekannteste Anbieter für Internettelefonie (Voice over IP, VoIP) ist zweifellos **Skype**. Die Installation und das Anlegen eines Account ist einfach. Man benötigt lediglich eine E-Mail Adresse. Skype-Verbindungen sind schwer zu blockieren. Die Client-Software findet fast immer eine Verbindung zum Netz, auch hinter restriktiven Firewalls. Skype bot eine gute Verschlüsselung und kann Verbindungen ins Festnetz und in Handynetze herstellen.

Nach der Übernahme von Skype durch Microsoft wurde die zensur-robuste Infrastruktur von Skype umgebaut und die Ende-zu-Ende Verschlüsselung von Skype kompromittiert. Statt einer Peer-to-Peer Infrastruktur nutzt Skype jetzt sogenannte Super-Nodes, die alle in Microsoft Rechenzentren stehen. Die Keys für die Verschlüsselung werden in der Microsoft Cloud hinterlegt und Microsoft nutzt nutzt die sich daraus ergebenden Möglichkeiten zum Mitlesen (juristisch korrekt wird in den Datenschutzbestimmungen darauf hingewiesen).

In einer Studie warnt das Fraunhofer-Institut für Eingebettete Systeme und Kommunikationstechnik (ESK) vor dem Einsatz von Skype in Unternehmen und Behörden:[1]

> *Auf Grund einiger Sicherheitsrisiken, welche die Nutzung von Skype mit sich bringt, wird der Telefondienst für den Austausch sicherheitsrelevanter und geschäftskritischer Informationen nicht empfohlen.*

Vielleicht ist Skype nur ein Beispiel für eine Gesetzmäßigkeit der Informationsgesellschaft? Kommunikationsdienste mit halbwegs guter Verschlüsselung werden kompromittiert, sobald sie eine hinreichend große Popularität erreicht haben. Unbeobachtete und private Kommunikation gibt es vielleicht nur in den Nischen von unterfinanzierten Open Source Projekten, die nur einer Gruppe von Nerds bekannt sind?

Abhörschnittstellen

Anfang der 90er Jehre des letzten Jahrhunderts wurde das Festnetz in den westlichen Industriestaaten digitalisiert und die GSM-Verschlüsselung für

[1] http://www.esk.fraunhofer.de/de/publikationen/studien/sykpe2.html

Handytelefonate wurde eingeführt. Klassische Abhörmaßnahmen für einen Telefonanschluss waren ohne Kooperation der Telekommuniationsanbieter und ohne vorbereitete Schnittstellen nicht mehr möglich.

Als Antwort auf diese Entwicklung wurden in allen westlichen Industriestaaten Gesetze beschlossen, die die Telekommunikationsanbieter zur Kooperation mit den Strafverfolgungsbehörden und Geheimdiensten verpflichten und Abhörschnittstellen zwingend vorschreiben. In den USA war es der *CALEA Act* [2] von 1994. In Deutschland wurde 1995 auf Initiative des Verfassungsschutz die *Fernmeldeverkehr-Überwachungsverordnung* (FÜV) [3] beschlossen, die 2002 durch die *Telekommunikations-Überwachungsverordnung* (TKÜV) [4] ersetzt wurde.

2005 wurde der CALEA Act durch das höchste US-Gericht so interpretiert, dass er auch für alle VoIP-Anbieter gilt, die Verbindungen in Telefonnetze weiterleiten können. Skype zierte sich anfangs, die geforderten Abhörschnittstellen zu implementieren. Mit der Übernahme von Skype durch Ebay im Nov. 2005 wurde die Diskussion beendet. Heute bietet Skype Abhörschnittstellen in allen westeuropäischen Ländern und zunehmend auch in anderen Ländern wie Indien. In Deutschland sind Abhörprotokolle aus Skype Gesprächen alltägliches Beweismaterial.[5]

Skype und andere VoIP-Anbieter, die Verbindungen in andere Telefonnetze herstellen können, sind in gleicher Weise abhörbar, wie Telefon oder Handy. Es ist albern, Skype als Spionagesoftware zu verdammen und gleichzeitig den ganzen Tag mit einem Smartphone rumzulaufen. Genauso ist eine Lüge, wenn man die Verbreitung von Skype als Grund für einen Staatstrojaner nennt.

10.1 Open Secure Telephony Network (OSTN)

Das Open Secure Telephony Network (OSTN) [6] wird vom Guardian Project entwickelt. Es bietet sichere Internettelefonie mit starker Ende-zu-Ende-Verschlüsselung, soll als Standard für Peer-2-Peer Telefonie ausgebaut werden und eine ähnlich einfache Nutzung wie Skype bieten.

Eine zentrale Rolle spielt das SRTP/ZRTP-Protokoll [7] von Phil Zimmermann, dem Erfinder von OpenPGP. Es gewährleistet eine sichere Ende-zu-Ende-Verschlüsselung der Sprachkommunikation. Wenn beide Kommunikationspartner eine Software verwenden, die das ZRPT-Protokoll beherrscht, wird die Verschlüsselung automatisch ausgehandelt. Daneben werden weitere etablierte Krypto-Protokolle genutzt.
Kurze Erläuterung der Begriffe:

[2] https://secure.wikimedia.org/wikipedia/en/wiki/Calea
[3] http://www.online-recht.de/vorges.html?FUEV
[4] https://de.wikipedia.org/wiki/Telekommunikations-%C3%9Cberwachungsverordnung
[5] http://www.lawblog.de/index.php/archives/2010/08/17/skype-staat-hort-mit
[6] https://guardianproject.info/wiki/OSTN
[7] https://tools.ietf.org/html/draft-zimmermann-avt-zrtp-22

SRTP definiert die Verschlüsselung des Sprachkanals. Die Verschlüsselung der Daten erfolgt symmetrische mit AES128/256 oder Twofish128/256. Für die Verschlüsselung wird ein gemeinsamer Schlüssel benötigt, der zuerst via ZRTP ausgehandelt wird.

ZRTP erledigt den Schlüsselaustausch für SRTP und nutzt dafür das Diffie-Helman Verfahren. Wenn beide VoIP-Clients ZRTP beherrschen, wird beim Aufbau der Verbindung ein Schlüssel für SRTP automatisch ausgehandelt und verwendet. Der Vorgang ist transparent und erfordert keine Aktionen der Nutzer. Allerdings könnte sich ein Man-in-the-Middle einschleichen, und die Verbindung kompromittieren (Belauschen).

SAS dient dem Schutz gegen Man-in-the-Middle Angriffe auf ZRTP. Den beiden Kommunikationspartnern wird eine 4-stellige Zeichenfolge angezeigt, die über den Sprachkanal zu verifizieren ist. Üblicherweise nennt der Anrufer die ersten beiden Buchstaben und der Angerufenen die beiden letzten Buchstaben. Wenn die Zeichenfolge identisch ist, kann man davon ausgehen, dass kein Man-in-the-Middle das Gespräch belauschen kann.

Damit bleibt als einziger Angriff auf die Kommunikation der Einsatz eines Trojaners, der das Gespräch vor der Verschlüsselung bzw. nach der Entschlüsselung abgreift. Dagegen kann man sich mit einer Live-DVD schützen.

10.1.1 OSTN-Provider

Um diese sichere Variante der Internettelefonie zu nutzen, benötigt man einen Account bei einem OSTN-kompatiblen Provider. Derzeit bietet nur Ostel.co[8]eine vollständige Umsetzuing von OSTN. Die Serversoftware OSTel ist Open Source, man kann auch seinen eigenen Server betreiben.

Die SRTP/ZRTP-Verschlüsselung ist ausschließlich von den Fähigkeiten der VoIP-Clients abhängig. Sie kann nicht nur mit den OSTN-Providern genutzt werden sondern auch mit Accounts bei anderen SIP-Providern wie z.B. linphone.org, Ekiga.net oder iptel.org. Allerdings vereinfacht OSTN die Konfiguration der Accounts im VoIP-Client.

VoIP-Clients mit OSTN-Support

Es gibt einige VoIP-Clients, die bereits die nötigen Voraussetzungen zur Nutzung von OSTN implementiert haben.

- Für den Desktop empfehle ich *Jitsi* [9], einen Java-basierter VoIP- und IM-Client für viele Betriebssysteme.
- *Linphone* kann unter Linux mit der Paketverwaltung installieren, es gibt inzwischen auch Versionen für Windows 10 und Android und iPhone Smartphones.[10]

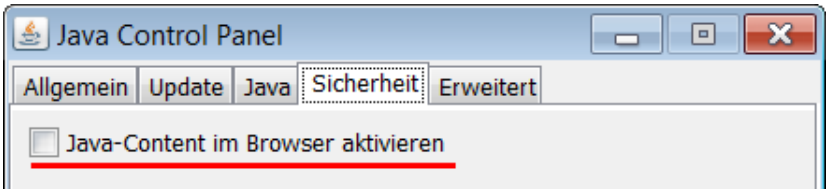
[8] https://ostel.co
[9] https://jitsi.org
[10] https://www.linphone.org

- Für Android-Smartphones ist *CSipSimple* [11] geeignet, das ebenfalls vom Guardian Project entwickelt wird.
- iPhone Nutzer können *Groundwire* [12] für $4,99 im App Store kaufen.

10.2 VoIP-Client Jitsi

Jitsi ist einen Java-basierter VoIP- und Instant Messaging Client für viele Betriebssysteme. Er unterstützt die SRTP/ZRTP-Verschlüsselung und das OSTN-Protokoll. Für die Installtion benötigt man zuerst einmal Java.

Java für Windows: Das Installationsprogramm für Java gibt auf der Webseite www.java.com[13]. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.



WICHTIG: Der Installer aktiviert auch ein Java-Plugin für alle Browser. Dieses Plug-in ist ein Sicherheitsrisiko und muss im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!

Java für Linux: Installieren Sie als erstes das Paket *default-jre* mit der Paketverwaltung der Distribution.

Jitsi installieren: Anschließend installiert man Jitsi, indem man das zum Betriebssystem passende Paket von der Downloadseite https://jitsi.org herunter lädt und als *Administrator* bzw. *root* installiert - fertig.

Hat man einen Account bei einem OSTN-Provider, dann muss man lediglich beim Start von Jitsi die Login Daten für den SIP-Account (Username und Passwort) eingeben, wie im Bild 10.1 dargestellt. Alle weiteren Einstellungen werden automatisch vorgenommen.

Wenn man einen Account beim SIP-Provider iptel.org hat, ist die Konfiguration ähnlich einfach. Man schließt den *Sign in* Dialog, wählt den Menüpunkt *File - Add new account* und in dem sich öffnenden Dialog als Netzwerk *iptel.org*. Jitsi enthält vorbereitete Einstellungen für diesen SIP-Provider.

[11] http://nightlies.csipsimple.com
[12] https://itunes.apple.com/us/app/groundwire-business-caliber/id378503081?mt=8
[13] http://www.java.com/de/

Abbildung 10.1: Account Daten eintragen

SAS Authentication

Bei einem verschlüsselten Gespräch wird beiden Teilnehmern eine Zeichenkette aus vier Buchstaben und Zahlen angezeigt. Diese Zeichenkette ist über den Sprachkanal mit dem Gegenüber zu verifizieren. Dabei nennt der Anrufer üblicherweise die ersten zwei Buchstaben und der Angerufene die letzten beiden Buchstaben bzw. Zahlen. Wenn beide Teilnehmer die gleiche Zeichenkette sehen, ist die Verbindung sicher verschlüsselt und unbeobachtet.

Anpassung der Konfiguration

Standardmäßig sind bei Jitsi viele Protokollierungen aktiv. In den den Einstellungen kann man diese Logfunktionen abschalten, um überflüssige Daten auf der Festplatte zu vermeiden.

Wer durch die Gerüchte über die Fortschritte der NSA beim Knacken von AES128 etwas verunsichert ist, kann in den Einstellungen des ZRTP Ninja die Verschlüsselung mit Twofish bevorzugen. Allerdings müssen beide Gesprächspartner diese Anpassung vornehmen.

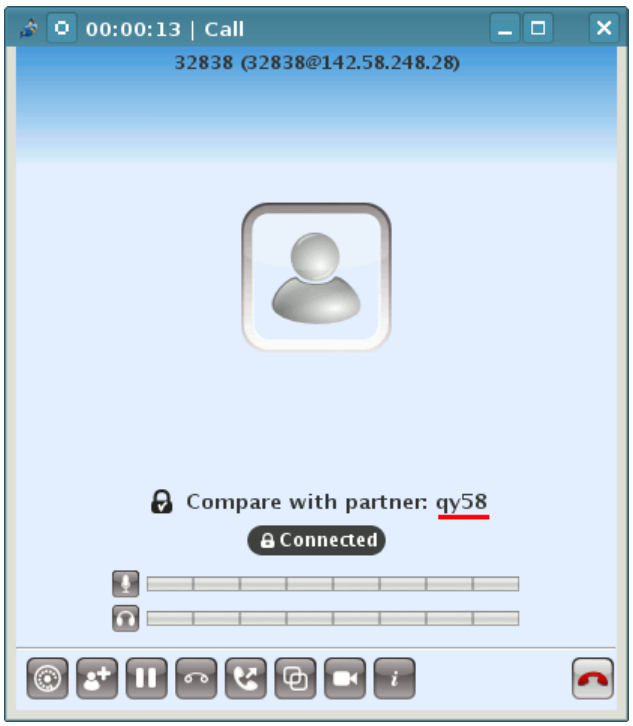


Abbildung 10.2: SAS Authentication

Kapitel 11

Anonymisierungsdienste

Anonymisierungsdienste verwischen die Spuren im Internet bei der Nutzung herkömmlicher Webdienste. Die verschlüsselte Kommunikation verhindert auch ein Belauschen des Datenverkehrs durch mitlesende Dritte. Diese Dienste sind für den anonymen Zugriff auf Websites geeignet und ermöglichen auch unbeobachtete, private Kommunikation via E-Mail, Jabber, IRC...

Die unbeobachtete, private Kommunikation schafft keine rechtsfreien Räume im Internet, wie Demagogen des Überwachungsstaates immer wieder behaupten. Sie ist ein grundlegendes Menschenrecht, das uns zusteht. Nach den Erfahrungen mit der Diktatur Mitte des letzten Jahrhunderts findet man dieses Grundrecht in allen übergeordneten Normenkatalogen, von der UN-Charta der Menschenrechte bis zum Grundgesetz.

Anonymisierungsdienste sind ein Hammer unter den Tools zur Verteidigung der Privatsphäre, aber nicht jedes Problem ist ein Nagel. Das Tracking von Anbietern wie DoubleClick verhindert man effektiver, indem man den Zugriff auf Werbung unterbindet. Anbieter wie z.B. Google erfordern es, Cookies und JavaScript im Browser zu kontrollieren. Anderenfalls wird man trotz Nutzung von Anonymisierungsdiensten identifiziert.

11.1 Warum sollte man diese Dienste nutzen?

Anonymisierungsdienste verstecken die IP-Adresse des Nutzers und verschlüsseln die Kommunikation zwischen Nutzer und den Servern des Dienstes. Außerdem werden spezifischer Merkmale modifiziert, die den Nutzer identifizieren könnten (Browser-Typ, Betriebssystem....).

1. **Profilbildung:** Nahezu alle großen Suchmaschinen generieren Profile von Nutzern, Facebook u.a. Anbieter speichern die IP-Adressen für Auswertungen. Nutzt man Anonymisierungsdienste, ist es nicht möglich, diese Information sinnvoll auszuwerten.

2. **Standortbestimmung:** Die Anbietern von Webdiensten können den Standort des Nutzers nicht via Geolocation bestimmen. Damit ist es nicht möglich:

- die Firma identifizieren, wenn der Nutzer in einem Firmennetz sitzt.
- bei mobiler Nutzung des Internet Bewegungsprofile zu erstellen.

3. **Belauschen durch Dritte:** Die verschlüsselte der Kommunikation mit den Servern des Anonymisierungsdienstes verhindert ein Mitlesen des Datenverkehrs durch Dritte in unsicheren Netzen. (Internet Cafes, WLANs am Flughafen oder im Hotel, TKÜV...)

4. **Rastern:** Obwohl IP-Adressen die Identifizierung von Nutzern ermöglichen, sind sie rechtlich in vielen Ländern ungenügend geschützt. In den USA können sie ohne richterliche Prüfung abgefragt werden. Die TK-Anbieter genießen Straffreiheit, wenn sie die nicht vorhandenen Grenzen übertreten. Wenig verwunderlich, dass man IP-Adressen zur täglichen Rasterfahndung nutzt. Facebook gibt täglich 10-20 IP-Adressen an US-Behörden, AOL übergibt 1000 Adressen pro Monat...

5. **Vorratsdatenspeicherung:** Ein Schreiben des Bundesdatenschutzbeauftragen an das Bundesverfassungsgericht macht viele unglaubliche Verstöße gegen die Nutzung der VDS-Daten offenkundig. Es werden häufig mehr Daten gespeichert, als gesetzlich vorgegeben. Auch die Bedarfsträger halten sich nicht an die Vorgaben des BVerfG.

   > Zitat: *So haben mir sämtliche Anbieter mitgeteilt, dass es recht häufig vorkomme, dass Beschlüsse nicht den formellen Anforderungen ...genügen. Wenn die Anbieter in derartigen Fällen entsprechenden Auskunftsersuchen nicht nachkämen, würde ihnen oft die Beschlagnahme von Servern oder die Vernehmung der leitenden Angestellten als Zeugen angedroht, um auf diesem Wege eine Auskunft zu erzwingen.*

   Die Telekom hat in zwei Monaten 2198 Anfragen beantwortet und dabei wahrscheinlich zu 70% auf VDS-Daten zurück gegriffen. Auch nachdem die Vorratsdatenspeicherung offiziell vom BVerfG beendet wurde, speichern alle Telekommunikationsanbieter weiterhin VDS-ähnliche Datenberge über mehrere Wochen.

6. **Zensur:** Der Datenverkehr kann vom Provider oder einer restriktiven Firewall nicht manipuliert oder blockiert werden. Anonymisierungsdienste ermöglichen einen unzensierten Zugang zum Internet. Sie können sowohl die "Great Firewall" von China und Mauretanien durchtunneln sowie die in westeuropäischen Ländern verbreitet Zensur durch Kompromittierung des DNS-Systems.

7. **Repressionen:** Blogger können Anonymisierungsdienste nutzen, um kritische Informationen aus ihrem Land zu verbreiten ohne die Gefahr persönlicher Repressionen zu riskieren. Für Blogger aus Südafrika, Syrien oder Burma ist es teilweise lebenswichtig, anonym zu bleiben. Iran wertet Twitter-Accounts aus, um Dissidenden zu beobachten

8. **Leimruten:** Einige Websites werden immer wieder als Honeypot genutzt. Ein Beispiel sind die Leimrute des BKA. In mehr als 150 Fällen wurden die Fahndungseiten von LKAs oder des BKA als Honeypot genutzt und

die Besucher der Webseiten in Ermittlungen einbezogen [1]. Surfer wurden identifiziert und machten sich verdächtig, wenn sie sich auffällig für bestimmte Themen interessieren.

9. **Geheimdienste:** Sicherheitsbehörden und Geheimdienste können mit diesen Diensten ihre Spuren verwischen. Nicht immer geht es dabei um aktuelle Operationen. Die Veröffentlichung der IP-Adressbereiche des BND bei Wikileaks ermöglichte interessante Schlussfolgerungen zur Arbeitsweise des Dienstes. Beispielsweise wurde damit bekannt, dass der BND gelegentlich einen bestimmten Escort Service in Berlin in Anspruch nimmt.

10. **Belauschen durch den Dienst:** Im Gegensatz zu einfachen VPNs oder Web-Proxys schützen die hier vorgestellten Anonymisierungsienste auch gegen Beobachtung durch die Betreiber des Dienstes selbst. Die mehrfache Verschlüsselung des Datenverkehrs und die Nutzung einer Kette von Servern verhindert, dass einzelne Betreiber des Dienstes die genutzten Webdienste einem Nutzer zuordnen können.

[1] http://heise.de/-1704448

11.2 Tor Onion Router

Das Onion Routing wurde von der US-Navy entwickelt. Die Weiterentwicklung liegt beim TorProject.org und wird durch Forschungsprojekte u.a. von deutschen Universitäten oder im Rahmen des *Google Summer of Code* unterstützt.

Tor nutzt ein weltweit verteiltes Netz von 6.000-7.000 aktiven Nodes. Aus diesem Pool werden jeweils 3 Nodes für eine Route ausgewählt. Die Route wechselt regelmäßig in kurzen Zeitabständen. Die zwiebelartige Verschlüsselung sichert die Anonymität der Kommunikation. Selbst wenn zwei Nodes einer Route kompromittiert wurden, ist eine Beobachtung durch mitlesende Dritte nicht möglich. Da die Route durch das Tor Netzwerk ständig wechselt, müsste ein großer Teil des Netzes kompromittiert worden sein, um einen Nutzer zuverlässig deanonymisieren zu können.

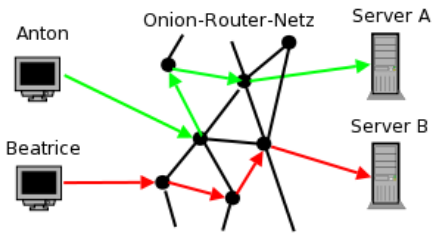


Abbildung 11.1: Prinzip von Tor

Tor ist neben Surfen auch für IRC, Instant-Messaging, den Abruf von Mailboxen oder Anderes nutzbar. Dabei versteckt Tor nur die IP-Adresse! Für die sichere Übertragung der Daten ist SSL- oder TLS-Verschlüsselung zu nutzen. Sonst besteht die Möglichkeit, dass sogenannte *Bad Exit Nodes* die Daten belauschen und an Userkennungen und Passwörter gelangen.

Der Inhalt der Kommunikation wird 1:1 übergeben. Für anonymes Surfen bedarf es weiterer Maßnahmen, um die Identifizierung anhand von Cookies, der HTTP-Header, ETags aus dem Cache oder Javascript zu verhindern. Das TorBrowserBundle ist für anonymes Surfen mit zu nutzen.

Verschiedene Sicherheitsforscher demonstrierten, dass es mit schnüffelnden *Bad Exit Nodes* relativ einfach möglich ist, Daten der Nutzer zu sammeln.

- Dan Egerstad demonstrierte, wie man in kurzer Zeit die Account Daten von mehr als 1000 E-Mail Postfächern erschnüffeln kann, u.a. von 200 Botschaften.[2]
- Auf der Black Hack 2009 wurde ein Angriff auf die HTTPS-Verschlüsselung beschrieben. In Webseiten wurden HTTPS-Links durch HTTP-Links ersetzt. Innerhalb von 24h konnten mit einen Tor Exit

[2] http://www.heise.de/security/news/meldung/95770

Node folgende Accounts erschnüffelt werden: 114x Yahoo, 50x GMail, 9x Paypal, 9x Linkedin, 3x Facebook.[3]

Im Februar 2012 haben mehrere russische Extis-Nodes diesen Angriff praktisch umgesetzt.

- Die Forscher um C. Castelluccia nutzten für ihren Aufsatz *Private Information Disclosure from Web Searches (The case of Google Web History)* einen schnüffelnden Tor Exit Node, um private Informationen von Google Nutzern zu gewinnen.[4]
- Um reale Zahlen für das Paper *Exploiting P2P Applications to Trace and Profile Tor Users* zu generieren, wurden 6 modifizierte Tor Nodes genutzt und innerhalb von 23 Tagen mehr als 10.000 User deanonymisiert.[5]

Man kann davon auszugehen, dass die Geheimdienste verschiedener Länder ebenfalls im Tor-Netz aktiv sind und sollte die Hinweise zur Sicherheit beachten: sensible Daten nur über SSL-verschlüsselte Verbindungen übertragen, SSL-Warnungen nicht einfach wegklicken, Cookies und Javascript deaktivieren... Dann ist Tor für anonyme Kommunikation geeignet.

Tor bietet nicht nur anonymen Zugriff auf verschiedene Services im Web. Die *Tor Hidden Services* bzw. *Tor Onion Sites* bieten Möglichkeiten, anonym und zensurresistent zu publizieren.

Finanzierung von Tor

Die Softwareentwicklung wird durch Spenden finanziert. TorProject.org benötigt pro Jahr ca. 1 Mio. Dollar für die Weiterentwicklung der Software und den Betrieb weniger Kernkomponenten des Dienstes. Die Grafik 11.2 zeigt die Zusammensetzung der Spender für 2009 (Quelle Tor Financial Report 2009).

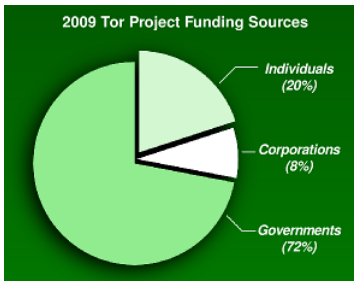


Abbildung 11.2: Anteil der Finanzierung von TorProject.org

Die Hauptsponsoren der NGOs, Companies und Einzelspender werden von TorProject.org auf der Webseite https://www.torproject.org/about/sponsors.html.en veröffentlicht. Der

[3] http://blog.internetnews.com/skerner/2009/02/black-hat-hacking-ssl-with-ssl.html
[4] http://planete.inrialpes.fr/projects/private-information-disclosure-from-web-searches/
[5] http://hal.inria.fr/inria-00574178/en/

große Anteil "Gouvernments" (72% der Einnahmen) kommt von US-Regierungsorganisationen und zu einem kleineren Teil von der schwedischen Regierung. Diese Spenden werden nicht einzeln aufgelistet.

Der Hauptteil der Infrastruktur wird von Enthusiasten finanziert und technisch in der Freizeit betreut. Die Kosten von 600-800 Euro pro Power-Server und Jahr sind als weitere Spenden anzusehen, die in der Grafik nicht erfasst sind. Die Administratoren ziehen keinen Vorteil aus ihrem Engagement, abgesehen von einem Zwiebel-T-Shirt.

Tor ist eine Triple-Use-Technik

Anonymisierungsdienste und Kryptografie allgemein sind Triple-Use-Techniken. Am Beispiel von Tor Onion Router kann man es deutlich erkennen:

1. Ganz normal Menschen nutzen Tor, um ihre Privatsphäre vor kommerziellen Datensammlern sowie staatlicher Überwachung und Repressalien zu schützen. Dieses Szenario der Nutzung steht häufig im Mittelpunkt der Diskussion unter Privacy Aktivisten, ist aber meiner Meinung nach die kleinste Nutzergruppe.

2. Kriminelle nutzen in großen Umfang Tor, um verschiedenste Formen der Kommunikation geheim zu halten. Beispielsweise verwenden Botnetze Tor, um die Kommunikation mit den C&C Servern geheim zu halten. Das bekannteste Beispiel ist das Mevade.A Botnet. Im Sommer 2013 waren zeitweise 80-90% der Tor Clients Mevade.A Bots, wie man in Bild 11.3 sehen kann.

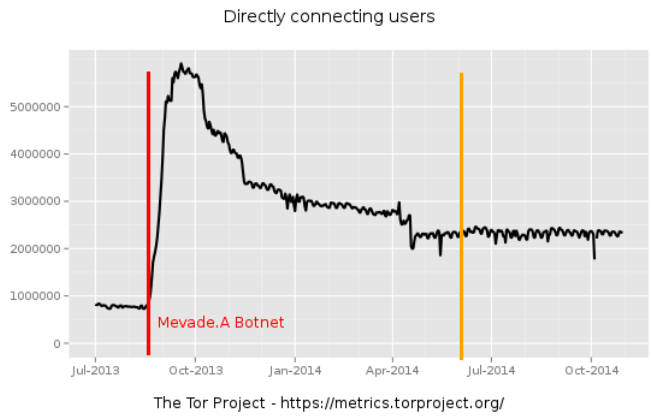


Abbildung 11.3: Mevada.A Botnetz von metrics.torproject.org

Außerdem nutzen Drogenhändler u.a. die Technik der Tor Onion Sites (Tor Hidden Services), um ihre Waren anzubieten. Im Rahmen der Operation Onymous konnte das FBI mehr als 400 Drogenmarkplätze abgeschalten werden. Das FBI hatte dabei technische Unterstützung von der Carnegie Mellon Unversity bei der Deanonymisierung von Tor

Onion Sites.

Die Nutzung von Anonymisierungsdiensten durch Kriminelle betrifft nicht nur Tor. Im Jahresbericht 2015 befürchten die Analysten von Europol, dass Kriminelle zukünfig das Invisible Internet Project (I2P) oder OpenBazaar statt Tor Onion Sites nutzen könnten, was die Verfolgung erschweren würde.

3. Die Geheimdienste nutzen Tor in erheblichen Umfang, um Kommunikation geheim zu halten. Außerdem ist Tor eine Waffe im Arsenal des US-Cybercommand. Im Frühjahr 2014 auf dem Höhepunkt der Ukraine-Krise wurde beispielsweise ein Botnetz in Russland hochgefahren, dass der russischen Gegenseite ernsthafte Probleme bereitet hat. In Bild 11.4 sieht man den Anstieg der Tor Nutzer in Russland (aber nicht international), der typisch für ein aktiviertes Botnetz ist. Die russische Regierung hat offiziell 4 Mio. Rubel für einen Exploit geboten um die beteiligten Tor Nodes zu deanonymiseren.

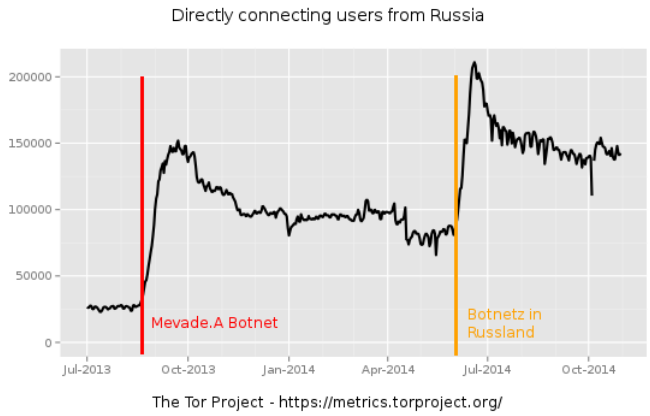


Abbildung 11.4: Botnetze mit Tor in Russland von metrics.torproject.org

Die Nutzung von Tor ist meiner Meinung nach ein **Spiegel der gesellschaftlichen Probleme** und nicht der Technik selbst anzulasten.

1. Das in der UN-Menschenrechtscharta und der Europäische Menschenrechtskonvention deklarierte Recht auf unbeobachtet, pivate Kommunikation ist durch die staatlich organisierte Massenüberwachung und kommerzielle Datensammlungen praktisch abgeschafft. Bundesinnenminister Friedrich empfiehlt Selbstschutz, weil die technischen Möglichkeiten zur Ausspähung nun einmal existieren (die Bankrotterklärung der Politik), und Tor ist ein Technik zum Selbstschutz.

2. Kriminaltät wie Wirtschaftskriminalität, Eigentumsdelikte, Drogenkriminalität... oder ganz allgm. *Handlungen im Widerspruch zu geltenden Gesetzen* sind gesellschaftliche Phänomene, für die man nicht den technischen Hilfsmitteln die Schuld geben kann.

3. Im Rahmen der erneuten Eskalation des *Kalten Krieges* wird jede Technik hinsichtlich Brauchbarkeit als Waffe geprüft. Tor war von Anfang ein Projekt der US-Army und wird deshalb von der US-Regierung finanziert. Auf der Webseite von TorProject.org wird diese Nutzung ausdrücklich beworben. Diese Verwendung sollte auch denen klar sein, die sich als freiwillige Unterstützer an der Finanzierung eines Tor Node beteiligen oder selbst einen Tor Node betreiben.

Durch diese unterschiedlichen Interessen entstehen skurrile Situationen, wenn das FBI der Carnegie Mellon Unversity 1 Mio. Dollar zur Verfügung stellt, um Tor Hidden Services für die Operation Onymous zu deanonymisieren[6], die Univerität die wiss. Ergebnisse auf der BlackHat Konferenz aber nicht publizieren darf[7], um die US-Cyberoperationen in Russland nicht zu gefährden, und die Entwickler bei TorProject.org auf Vermutungen angewiesen sind[8], um die Bugs zu fixen, damit sie politischen Aktivisten wie Wikileaks eine vertrauenswürdige Infrastruktur bereit stellen können.

11.2.1 Security Notes

Die Sicherheit von IP-Anonymisierern wie Tor Oinion Router ergibt sich nicht alleine aus der Qualität der Anonymisierungssoftware und der Kryptografie. Durch Fehler in der Anwendung oder durch falsche Konfiguration kann die Anonymität komplett ausgehebelt werden.

- Wer in seinem Standardbrowser nur die Proxy-Einstellungen anpasst um Tor zu verwenden, ist auch nicht sicher anonym. Eine Deanonymisierung ist mit WebRTC sowie Flash- oder Java-Applets möglich. Cookies und andere Trackingfeatures können langfristig ebenfalls zu einer Deanonymisierung des Surfverhaltens führen.

- Viele Jabber Clients (XMPP) anonymisieren DNS-Requests nicht. Der IM-Client Pidgin hat außerdem Probleme mit Voice- und Video-Chats. Die Proxy-Einstellungen werden bei Voice- und Video-Chats umgangen und es ist möglich, einen User mit einer Einladung zum Voice-Chat zu deanonymisieren.

- Einige Protolle übertragen die IP-Adresse des eigenen Rechners zusätzlich in Headern des Protokoll-Stacks. Ein Beispiel dafür sind nicht-anonyme Peer-2-Peer Protokolle wie BitTorrent. Damit ist es ebenfalls möglich, User zu deanonymisieren. Eine wissenschaftliche Arbeit zeigt, wie 10.000 BitTorrent Nutzer via Tor deanomisiert werden konnten.

- Durch Software aus fragwürdigen Quellen können Backdoors zur Deanonymisierung geöffnet werden. Eine Gruppe von ANONYMOUS demonstrierte es, indem sie eine modifizierte Version des Firefox Add-on TorButton zum Download anboten, dass wirklich von einigen Tor-Nutzern verwendet wurde. Dieses Add-on enthielt eine Backdoor, um die Nutzer von einigen Tor Hidden Services mit kinderpronografischem

[6] https://blog.torproject.org/blog/did-fbi-pay-university-attack-tor-users
[7] https://web.archive.org/web/20140705114447/http://blackhat.com/us-14/briefings.html
[8] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/

Material zu identifizieren. Die Liste der damit deanonymisierten Surfer wurde im Herbst 2011 im Internet veröffentlicht.

Schlussfolgerungen:

- TorProject empfiehlt für anonymes Surfen ausdrücklich das TorBrowser-Bundle. Das ist eine angepasste Version des Browser Mozilla Firefox zusammen mit dem Tor Daemon. Nur diese Konfiguration kann als wirklich sicher nach dem aktuellen Stand der Technik gelten. Die vielen Sicherheitseinstellungen dieser Softwarekombination kann man nur unvollständig selbst umsetzen.
- Für alle weiteren Anwendungen sind die Anleitungen der Projekte zu lesen und zu respektieren. Nur die von den Entwicklern als sicher deklarierten Anwendungen sollten mit Tor genutzt werden.
- Verwenden Sie ausschießlich die Originalsoftware der Entwickler.

11.2.2 Anonym Surfen mit dem TorBrowserBundle

Das TorBrowserBundle enthält einen modifizierten Firefox als Browser sowie den Tor Daemon und ein Control Panel. Die Webseite stellt das TorBrowser-Bundle für verschiedene Betriebssysteme und in unterschiedlichen Sprachen zur Verfügung.

HINWEIS: wir empfehlen ausdrücklich, die **englische Version des Tor-Browsers (en-US)** herunter zu laden. In den letzten Jahren gab es immer wieder aufgrund von Bugs im TBB die Möglichkeit, Hinweise auf die Lokalisierung des Browser zu fimden, z.B via Javascript *date.tolocale()* Funktion (Bug #5926) oder via Informationen aus dem HTTP Accept-Language Header (Bug #628) oder via *ressource://* URI (Bug #8725). Wenn man die deutsch lokalisierte Version des TorBrowsers nutzt, gibt man möglicherweise einen Hinweis auf eine deutsche Herkunft, und das möchte man beim anonymen Surfen natürlich vermeiden.

Neben der stabilen Version des TorBrowserBundle bietet TorProject.org auch eine Alpha-Version mit neuen Features zum Testen an. Diese Versionen enthalten manchmal Features, die man sich als Anwender sehr wünscht. Für den produktiven Einsatz empfehlen wir aber trotzdem, die stabile Version zu nutzen und zu warten, bis die Entwickler die neuen Features als ausreichend getestet einstufen und in die stabile Version übernehmen. Neben den möglichen Problemen der Stabilität ist auch höhere Anonymität ein Grund für die Empfehlung, da die Anonymitätsgruppe mit der stabilen Version größer ist.

Installation

Das Archiv ist nach dem Download zu entpacken, keine Installation nötig.

- Unter Windows öffnet man nach dem Download das selbstentpackende Archiv mit einem Doppelklick im Dateimanager und wählt ein Zielverzeichnis. Nach dem Entpacken startet man alle Komponenten mit einem Doppelklick auf **Start Tor Browser.exe** im Dateimanager.

- Unter Linux entpackt man das Archiv mit dem bevorzugten Archiv-Manager oder erledigt es auf der Kommandozeile mit:

  ```
  > tar -xaf tor-browser-*
  ```

  Danach kann man das TorBrowserBundle starten, indem man das Startscript auf der Kommandozeile aufruft oder mit einem Klick im Dateimanager startet:

  ```
  > tor-browser_en-US/start-tor-browser.desktop
  ```

  Mit einem kleinen Kommando kann man den TorBrowser im Startmenü des Desktops in der Programmgruppe *Internet* hinzufügen, um zukünftig den Start zu vereinfachen:

  ```
  > tor-browser_en-US/start-tor-browser.desktop --register-app
  ```

- Für Debian und Ubuntu Derivate gibt es außerdem den *TorBrowser Launcher*, der sich um Download, Verifikation und Installation des TorBrowserBundles kümmert. Das Paket kann man mit dem bevorzugten Paketmanager installieren:

  ```
  > sudo apt install torbrowser-launcher
  ```

  In der Regel wird auch gleich ein Tor Daemon installiert. Diesen Tor Daemon braucht man evtl. nur für den ersten, initialen Download des TorBrowserBundle. Es ist aber kein Sicherheitsgewinn, wenn man das TorBrowserBundle via Tor herunter lädt und man kann diesen Tor Daemon gleich wieder entfernen, da das TorBrowserBundle eine aktuellere Version von Tor enthält.

  ```
  > sudo apt purge tor
  ```

  In der Programmgruppe *Internet* findet man zwei neue Menüpunkte. Wenn man den Menüpunkt *TorBrowser Launcher Settings* wählt, öffnet sich das in Bild 11.5 gezeigte Fenster. Den *Download over System Tor* kann man deaktivieren, man sollte die englische Version des TorBrowsers herunterladen und außerdem kann man einen Mirror wählen, falls die Webseite von TorProject.org nicht erreichbar ist. Ein Klick auf den *Install Button* lädt das TorBrowserBundle herunter, verifiziert die OpenPGP Signatur und installiert den TorBrowser. Zum Starten verwendet man zukünftig den Menüpunkt *TorBrowser* in der Programmgruppe *Internet*.

Wenn die Downloadseite für das TorBrowserBundle gesperrt ist, dann findet man unter GetTor[9] alternative Downloadmöglichkeiten. Man kann z.B. per Jabber/XMPP oder E-Mail eine Nachricht mit dem gewünschten Betriebssystem (windows, linux, osx) an den Account *gettor@torproject.org* schicken und bekommt eine Liste alternativer Downloadlinks.

[9] https://gettor.torproject.org/

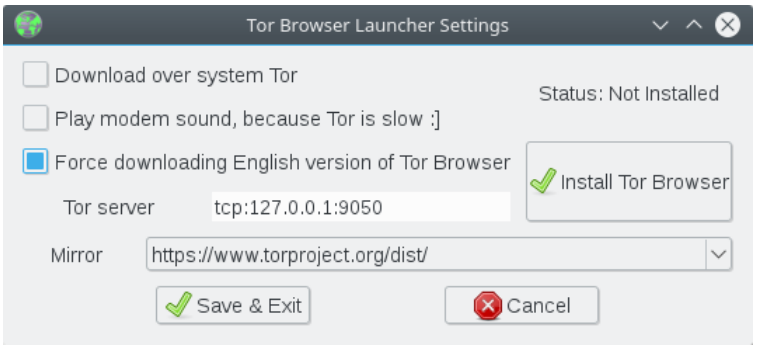


Abbildung 11.5: Start des TorBrowser

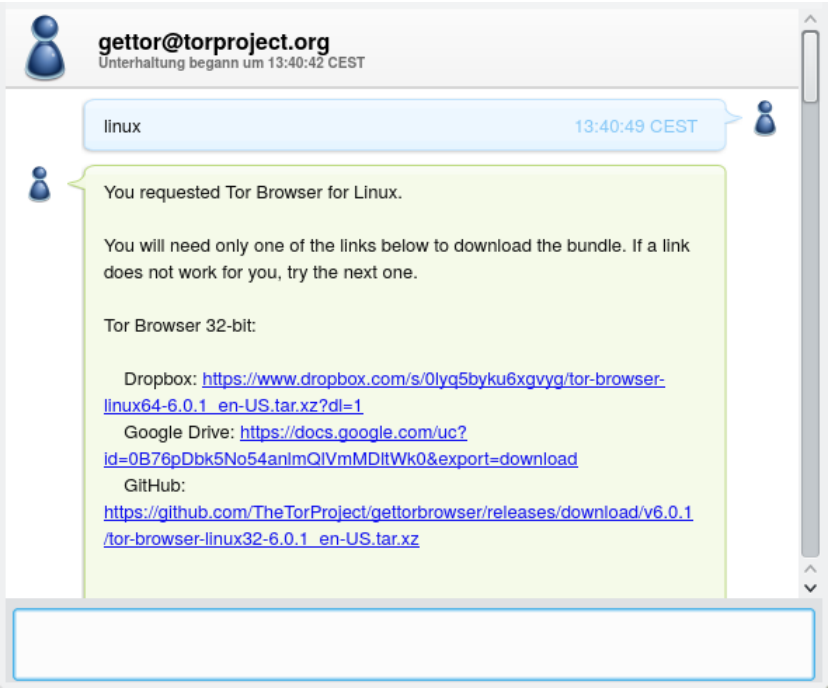


Abbildung 11.6: Alternative Downloadlinks via Jabber/XMPP abrufen

Abbildung 11.7: Start des TorBrowser

Beim ersten Start öffnet sich zuerst das Control Panel. Hier kann man bei Problemen Einstellungen zur Umgehung von Firewalls konfigurieren (z.B. wenn eine Firewall nur Verbindungen zu bestimmten Ports passieren lässt) oder man kann den Tor Daemon mit Klick auf den Button *Verbinde* ohne weitere Konfiguration starten.

Größe des Browserfensters

Der TorBrowser startet mit einer festgelegten Größe des Browserfensters. Die Fensterbreite sollte ein Vielfaches von 200px sein (max. 1000px) und die Höhe ein Vielfaches von 100px. Die Fenstergröße wird gleichzeitig als Bildschirmgröße via Javascript bereitgestellt. Da die innere Größe des Browserfensters und die Bildschirmgröße als Tracking-Feature genutzt werden, sollte man die voreingestellte Größe des Browserfensters nicht(!) ändern.

Sicherheitseinstellungen

Rule 41 of the US Federal Rules of Criminal Procedure[10] erlaubt seit Dez. 2016 dem FBI das massenweise Hacken von Tor- und VPN-Nutzern unabhägig davon, in welchem Land die Tor-Nutzer sich befinden. Kann das FBI den TorBrowser hacken und unbemerkt einen Tojaner installieren? Ja.

[10] https://blog.torproject.org/blog/day-action-stop-changes-rule-41

1. 2015 verwendete das FBI einen Zero-Day-Exploit im TorBrowser, um einen Trojaner zu installieren und die Tor-Nutzer damit zu deanonymisieren. Welcher Lücke im Firefox dabei ausgenutzt wurde, ist nicht bekannt. Mozilla und TorProject.org haben sich bemüht, aber die Informationen zur ausgenutzten Lücke wurden unter Hinweis auf die Nationale Sicherheit als geheim eingestuft.[11]

2. Im Sommer 2013 wurden tausende Tor-Nutzer mit dem FBI-Trojaner *Magneto* infiziert. Der Exploit zur Installation des Trojaners nutzte einen Javascript Bug im TorBrowser aus. Der installierte Trojaner sendete die IP-Adresse, die MAC-Adresse und den Namen des Rechners an einen FBI Server, um den Tor-Nutzer zu deanonymisieren.[12]

3. Aus den Snwoden Dokumenten geht hervor, dass die NSA das TorBrowserBundle auf Basis von Firefox 10 esr über einen Bug in E4X, einer XML Extension für Javascript, automatisiert angreifen und Nutzer deanonymisieren konnten.[13]

4. Außerdem geht aus den Snwoden Dokumenten hervor, dass die NSA eine *QUANTUMCOOKIE insert attack* aktiv nutzt, um Tor Nutzer zu deanonymisieren.[14]

Die Tor-Entwickler haben den Tradeoff zwischen einfacher Benutzbarkeit und Sicherheit in den Default-Einstellungen zugunsten der einfachen Benutzbarkeit entschieden. Es wird aber auch anerkannt, dass diese Einstellungen ein Sicherheitrisiko sind. In den FAQ steht:

> *There's a tradeoff here. On the one hand, we should leave JavaScript enabled by default so websites work the way users expect. On the other hand, we should disable JavaScript by default to better protect against browser vulnerabilities (not just a theoretical concern!).*

Beim Start wird man darauf hingewiesen, dass man die Sicherheitseinstellungen anpassen kann. TorBrowser startet standardmäßig mit dem niedrigsten Sicherheitslevel *niedrig*, um das Surferlebnis möglichst wenig einzuschränken. Bei Bedarf kann man den Sicherheitslevel erhöhen. Wir empfehle den umgekehrten Weg. Meiner Meinung nach sollte man den Sicherheitslevel auf *hoch* setzen und nur auf *Mittel* verringern, wenn es für die Nutzung einer (vertrauenswürdigen) Webseite nötig ist und wenn diese Webseite via HTTPS oder als Tor Hidden Service geladen wurde. Fast alle Websites, die einen Login erfordern (E-Mail Provider u.ä.), kann man mit dem Sicherheitslevel *Mittel* ohne Einschränkungen nutzen.

Wenn man die Sicherheitseinstellungen weiter verringert, könnten bösartige Exit Nodes unschöne Dinge in den HTML Code einer Webseite einfügen, die unverschlüsselt via HTTP geladen wird.

[11] https://motherboard.vice.com/read/the-fbi-is-classifying-its-tor-browser-exploit
[12] http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi
[13] http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity
[14] http://www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/

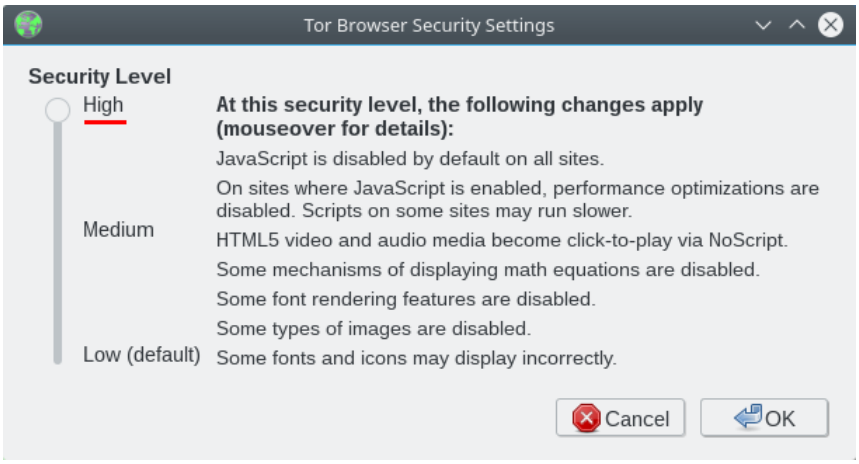


Abbildung 11.8: Sicherheitslevel im TorBrowser anpassen

Abbildung 11.9: Neue Identät im TorBrowser wählen

Cookies und EverCookies

Alle Cookies und alle bekannten EverCookie Markierungen werden beim Beenden des TorBrowsers gelöscht oder wenn man den Menüpunkt *Neue Identität* der Zwiebel in der Toolbar wählt (Bild 11.9). Man sollte dem Anonymitätskonzept des TorBrowser folgen und bei Bedarf gelegentlich alle Identifikationsmerkmale löschen. Insbesondere vor und nach dem Login bei einem Webdienst sollte man alle Markierungen entfernen, um eine Verknüpfung des Surfverhaltens mit Accountdaten zu verhindern.

PDFs und andere Dokumente

Auf der Downloadseite des TorBrowserBundles findet man unten einige Sicherheitshinweise[15], unter anderem zu PDFs und anderen Dokumenten:

[15] https://www.torproject.org/download/download

> ***Don't open documents downloaded through Tor while online***
>
> *You should be very careful when downloading documents via Tor (especially DOC and PDF files) as these documents can contain Internet resources that will be downloaded outside of Tor by the application that opens them. This will reveal your non-Tor IP address.*
>
> ***If you must work with DOC and/or PDF files, we strongly recommend either using a disconnected computer**, downloading the free VirtualBox and using it with a virtual machine image with networking disabled, or using Tails.*

PDFs und andere Office Dokumente können Tracking Wanzen enthalten, die beim Öffnen des Dokumentes von einem Server geladen werden. Wenn man sie in einem PDF-Reader öffnet, während man online ist, dann kann man deanonmisert werden. Standardmäßig öffnet TorBrowser PDFs im eigenen Viewer PDF.js. Damit sollte man zwar nicht deanonymisiert werden können, aber der Server kann zumindest das Öffnen des Dokumentes registrieren, auch nicht schön. Außerdem gibt es immer wieder Bug in Mozillas PDF.js, die für einen Exploit genutzt werden können (z.B. mfsa2015-69 vom Juli 2015).

Um nicht immer daran denken zu müssen, mit der rechten Maustaste auf einen PDF-Link zu klicken und *Speichern unter...* zu wählen, empfehle ich, die Einstellung im TorBrowser für PDF-Dokumente zu ändern und auf *Speichern* zu setzen.

Die via Tor herunter geladenen Dokumente kann man in einem besonderen Ordner speichern. Dann behält man den Überblick und weiss, dass man diese Dokumente nur öffnen darf, wenn man den Netzwerkstecker gezogen hat oder die WLAN-Verbindung ausgeschaltet wurde.

Mit dem Metadata Anonymisation Toolkit (MAT) kann man PDF-Dokumente nach dem Download säubern. Die Technik von MAT garantiert, dass die Tracking Wanzen entschärft werden und nicht mehr spionieren können. Die gesäuberten PDFs kann man gefahrlos im Online-Modus öffnen und weitergeben.

11.2.3 Tor Hidden Services

Das Tor Netzwerk ermöglicht nicht nur den anonymen Zugriff auf herkömmliche Angebote im Web sondern auch die Bereitstellung anonymer, zensurresitenter und schwer lokalisierbarer Angebote auf den Tor-Nodes. Der Zugriff auf die Tor Hidden Services (Neu: Tor Onion Sites) ist nur über das Tor Netzwerk möglich. Eine kryptische Adresse mit der Top-Level Domain .onion dient gleichzeitig als Hashwert für ein System von Schlüsseln, welches sicherstellt, dass der Nutzer auch wirklich mit dem gewünschten Dienst verbunden wird. Die vollständige Anonymisierung des Datenverkehrs stellt sicher, dass auch die Betreiber nur sehr schwer ermittelt werden können.

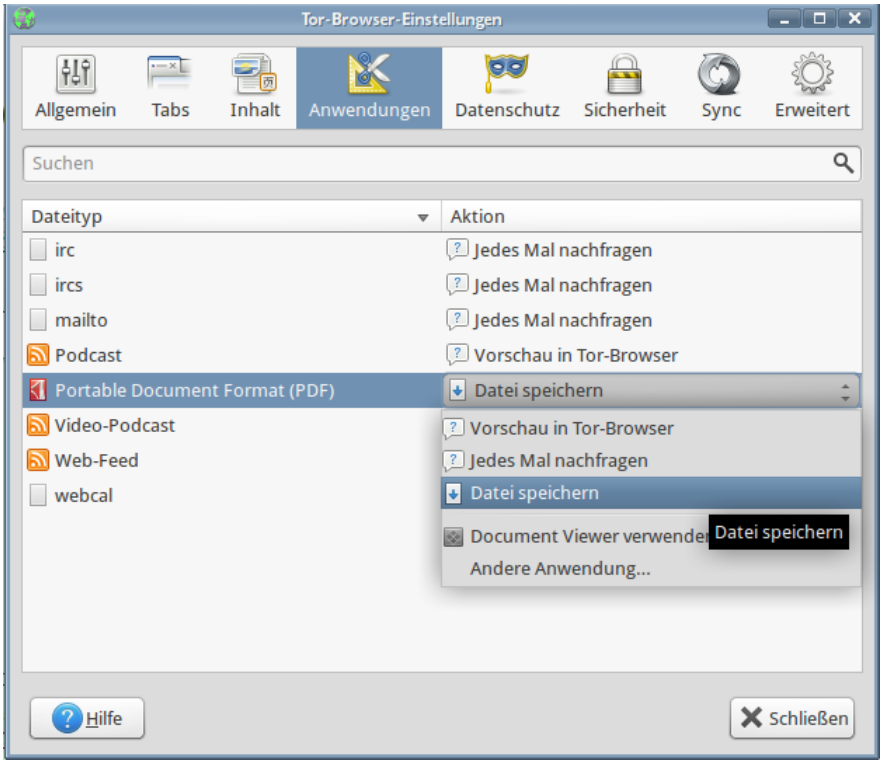


Abbildung 11.10: Einstellungen für PDF-Dokumente im TorBrowser

Tor Hidden Services als Alternative

Es gibt mehere Angebote im normalen Web, die zusätzlich als Tor Hidden Service bzw. als Tor Onion Site anonym und unbeobachtet erreichbar sind. Wenn man Tor nutzt, sollte man diese Hidden Services den normalen Webadressen vorziehen, da dann keine Gefahr durch Bad Tor Exit Nodes besteht.

- Die Suchmaschine *DuckDuckGo* ist auch als Tor Onion Site unter der Adresse http://3g2upl4pq6kufc4m.onion zu finden und die Suchmaschine Metager unter http://b7cxf4dkdsko6ah2.onion/tor/. Für Firefox gibt es bei Mycroft Add-ons für die Suchleiste, das diese Hidden Services nutzen. Metager (deutsche Suchmaschine) ist unter http://b7cxf4dkdsko6ah2.onion zu finden.
- Die folgenden Webseiten können als Tor Onion Sites aufgerufen werden:
  - TorProject.org ist unter http://expyuzz4wqqyqhjn.onion erreichbar. Weitere Onion Sites von TorProject.org findet man auf der Übersichtsseite https://onion.torproject.org bzw. auf der Tor Onion Site http:/yz7lpwfhhzcdyc5y.onion.
  - Das Debian Projekt bietet eine Tor Onion Site für die Hauptseite unter http://sejnfjrq6szgca7v.onion und weitere Tor Onion Sites für einige Projekte an. Eine Übersicht findet man unter https://onion.debian.org bzw. http://5nca3wxl33tzlzj5.onion.
  - Wikileaks bietet eine Submission Plattform für Uploads unter http://wlupld3ptjvsgwqw.onion und einen sicheren Webchat unter http://wlchatc3pjwpli5r.onion.
  - Heise.de bietet einen sicheren Briefkasten auf Basis von Secure Drop für Tippgeber (sogenannte Whistleblower) unter http://sq4lecqyx4izcpkp.onion.
- Die folgenden E-Mail Provider bieten POP3, IMAP und SMTP auch als Hidden Service an:
  - Mailbox.org: unter kqiafglit242fygz.onion[16]
  - JPBerlin.de: unter 63itrelmlq7jvmwp.onion
  - Riseup.net: unter zsolxunfmbfuq7wf.onion[17]
- Die folgenden Jabber-Server sind als Tor Hidden Service erreichbar:
  - jabber-germany.de unter dbbrphko5tqcpar3.onion[18]
  - CalyxInstitut.org unter ijeeynrc6x2uy5ob.onion[19]
  - Mailbox.org unter kqiafglit242fygz.onion[20]
  - systemli.org unter x5tno6mwkncu5m3h.onion[21]

[16] https://support.mailbox.org/knowledge-base/article/der-tor-exit-node-von-mailbox-org
[17] https://help.riseup.net/en/tor
[18] https://www.jabber-germany.de
[19] https://calyxinstitute.org/projects/public_jabber_xmpp_server
[20] https://support.mailbox.org/knowledge-base/article/tormessenger-fuer-mailbox-org-konfigurieren
[21] https://www.systemli.org/en/service/xmpp.html

  - Riseup.net unter 4cjw6cwpeaeppfqz.onion[22]
  - securejabber.me unter giyvshdnojeivkom.onion[23]
  - jabber.otr.im unter 5rgdtlawqkcplz75.onion[24]
  - jabber.so36.net unter s4fgy24e2b5weqdb.onion[25]
  - creep.im unter creep7nissfumwyx.onion[26]
  - Draugr.de unter jfel5icoxf3nmftl.onion[27]
  - Trashserver.net unter m4c722bvc2r7brnn.onion[28]
  - Jabber.cat unter sybzodlxacch7st7[29]
  - tchncs.de unter duvfmyqmdlyvc3mi.onion[30]

- Das SILC-Netz des CCC Dresden ist unter t3oisyiugzgvxph5.onion erreichbar.

- Das Freenode IRC-Netzwerk kann als Tor Hidden Service unter der Adresse p4fsi4ockecnea7l.onion (Port: 6667) genutzt werden (nur mit registriertem Nick!)

- HKP-Keyserver für OpenPGP Schlüssel sind unter folgenden Adressen erreichbar:

  - SKS Keyserver Pool: hkp://jirk5u4osbsr34t5.onion
  - keys.indymedia.org: hkp://qtt2yl5jocgrk7nu.onion
  - TorBirdy verwendet: hkp://qdigse2yzvuglcix.onion

Tor Hidden Services für E-Mail Kommunikation

Für unbeobachtete Kommunikation gibt es folgenden Dienste, die ausschließlich aus Tor Hidden Service genutzt werden können:

- Das *Lelantos-Project* ist ein E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse http://lelantoss7bcnwbv.onion betrieben wird. Für einen E-Mail Account muss man mit Bitcoins bezahlen, Gateway ins normale Web ist vorhanden.

- *Mail2Tor* ist ein weiterer E-Mail Dienst, der von Unbekannten als Tor Hidden Service unter der Adresse http://mail2tor2zyjdctd.onion betrieben wird. Accounts sind kostenlos, E-Mail können ebenfalls ins normale Internet gesendet und von dort empfangen werden.

[22] https://help.riseup.net/en/tor
[23] https://securejabber.me
[24] https://www.otr.im/chat.html
[25] https://www.so36.net/services/xmpp
[26] https://creep.im
[27] https://www.draugr.de/neues/Tor_Hidden_Service
[28] https://trashserver.net/technik
[29] https://jabber.cat/deutsch.html
[30] https://tchncs.de/xmpp

- *SIGAINT* ist ein kostenfreier E-Mail Service mit kostenpflichtigem Premium Angebot unter der Adresse http://sigaintevyh2rzvw.onion. Die kostenfreie Version bietet nur ein Webmail Interface. SMTP/POP3/IMAP für die Nutzung mit Thunderbird + TorBirdy gibt es nur für Premium Kunden. E-Mails können ebenfalls ins normale Internet gesendet und von dort empfangen werden.

- *TorBox* ist ein kostenfreier Hidden-only E-Mail Service und unter Adresse http://torbox3uiot6wchz.onion erreichbar. Es können keine E-Mails ins normale Internet gesendet oder von dort empfangen werden.

Debian GNU/Linux Hidden Software Repository

Für Debian GNU/Linux gibt es einen Mirror der Repositories als Tor Hidden Service unter der Adresse *vwakviie2ienjx6t.onion*. Außerdem gibt es den Apt-Transport-Tor, der die Nutzung des Hidden Service mit den ganz normalen Tools zur Softwareverwaltung ermöglicht. Um die Software des Systems anonym und von Dritten unbeobachtet zu verwalten und zu aktualisieren ist ab Debian *jessie* nur das Paket *apt-transport-tor* zu installieren:

```
> sudo apt install apt-transport-tor
```

Anschließend editiert man die Datei */etc/apt/sources.list* und ersetzt die Server für Debian Paketquellen nach folgendem Muster:

```
deb tor+http://vwakviie2ienjx6t.onion/debian jessie
deb tor+http://vwakviie2ienjx6t.onion/debian jessie-updates main
deb tor+http://sgvtcaew4bxjd7ln.onion/debian-security jessie/updates main

# deb tor+http://vwakviie2ienjx6t.onion/debian jessie-backports main
```

Zukünftig nutzen alle Tools zur Softwareverwaltung (aptitude, Synaptic, KPackekit, ...) den Tor Hidden Service für die Installation und Aktualisierung der Software.

Sonstiges

Ansonsten kenne ich kaum etwas, dass ich weiterempfehlen möchte. Meine "Sammlung" an reinen Tor Hidden Services enthält:

- 34x Angebote, die kinderpornografischen Schmutz zum Download anbieten (ausschließlich und teilweise zusätzlich zu anderen Inhalten). Das BKA hat eine etwas umfangreichere Liste mit 545 Seiten (Stand: 2012).[31]

- 3x Angebote zum Thema *Rent a Killer*. Ein Auftragsmord kostet offenbar nur 20.000 Dollar (wenn diese Angebote echt sind).

- Ein Angebot für gefakete Ausweisdokumente (aufgrund der mit Photoshop o.ä. bearbeiteten Screenshots der Beispieldokumente auf der Webseite halte ich das Angebot selbst für einen Fake).

[31] http://heise.de/-2124930

- Mehrere Handelsplattformen für Drogen. (Das FBI kannte über 400 Plattformen zu diesem Thema.)
- Einige gähnend langweilige Foren & Blogs mit 2-3 Beiträgen pro Monat.
- Einige Index-Seiten mit Listen für verfügbare Hidden Services wie das legendäre *HiddenWiki* oder das neuere *TorDirectory*. In diesen Index Listen findet man massenweise Verweise auf Angebote mit Bezeichnungen wie *TorPedo*, *PedoVideoUpload*, *PedoImages*. Nach Beobachtung von ANONYMOUS sollen 70% der Besucher des *HiddenWiki* die Adult Section aufsuchen, wo dieses Schmutzzeug verlinkt ist.

In dem Paper *Cryptopolitik and the Darknet* (2016) haben sich die Autoren D. Moore und T. Rid empirisch mit den Tor Onion Sites beschäftigt. Von den 2723 besuchten Onion Sites waren 1547 Onion Sites auf kriminelle, illegale Aktivitäten ausgerichtet.[32]

Fake Onion Sites

Für Tor Onion Sites gibt es kein Vertrauens- oder Reputationsmodell. Es ist unbekannt, wer einen Tor Hidden Services betreibt und es ist damit sehr einfach, Honeypots aufzusetzen. Die kryptischen Adressen sind nur schwer verifizierbar. Das Problem von *Anonymität und Reputation* ist im Kapitel *Nachdenken* ausführlicher beschrieben.

Juha Nurmi (Betreiber der Hidden Service Suchmaschine Ahmia.fi) veröffentlichte bereits zwei Warnungen im Juni 2015[33] und Januar 2016[34] mit 300 Fake Onion Sites, die den originalen Onion Sites täuschend ähnlich sehen. Diese Fake Sites leiten des Traffic der originalen Sites durch, modifizieren die Daten geringfühig oder erschnüffeln Login Credentials.

Auch Suchmaschinen mit Hidden Service Adressen wie DuckDuckGo (Tor) und Ahmia.fi waren betroffen, wie die Sceenshots in Bild 11.11 zeigen. Die Fake Site sieht dem Original täuschend ähnlich, die Besucher werden mit den Suchergebnissen aber auf andere Fake Onion Sites gelenkt.

Teilweise sind die Adressen der Fake Sites den Originalen sehr ähnlich:

```
REAL: http://torlinkbgs6aabns.onion
FAKE: http://torlinksb7apugxr.onion

REAL: http://valhallaxmn3fydu.onion
FAKE: http://valhalla4qb6qccm.onion

REAL: http://vendor7zqdpty4oo.onion
FAKE: http://vendor7eewu66mcc.onion
```

[32] http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085
[33] https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html
[34] https://lists.torproject.org/pipermail/tor-talk/2016-January/040038.html

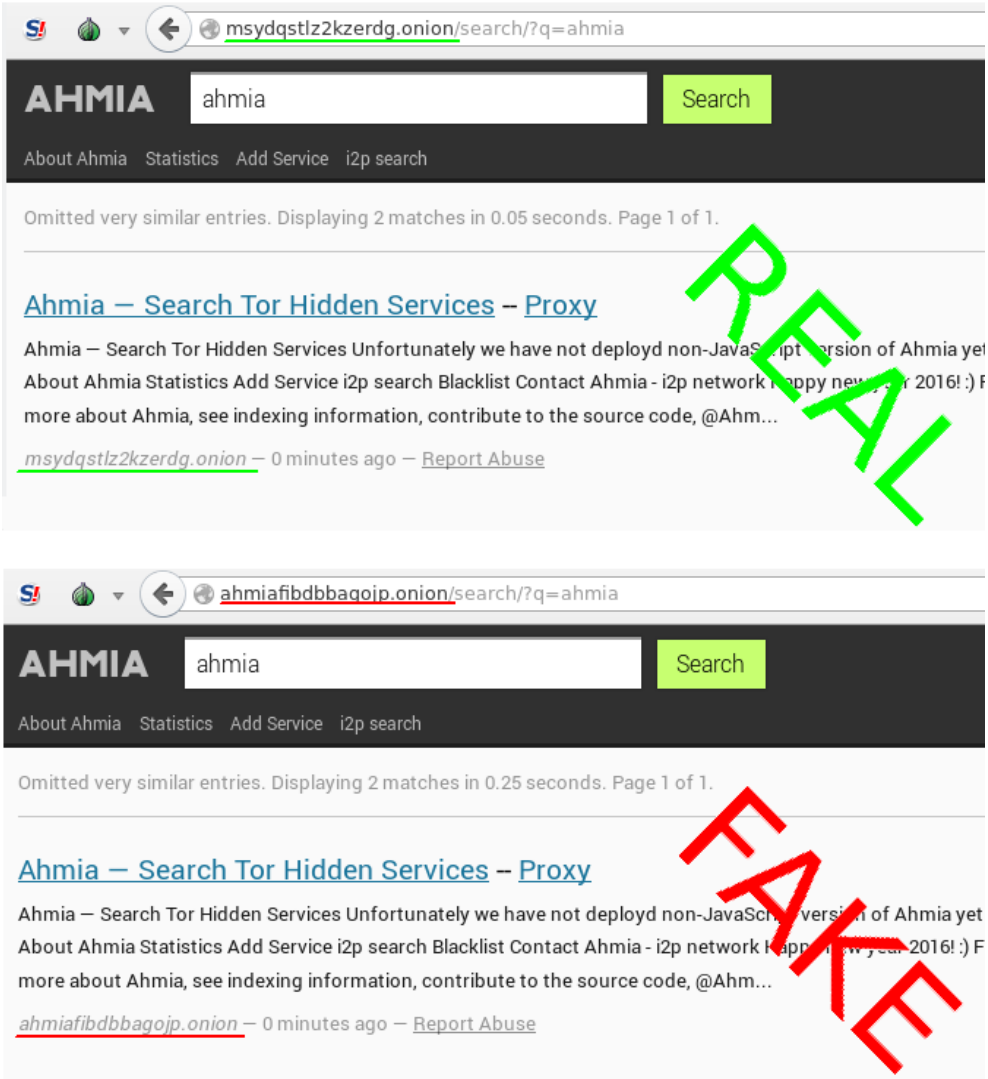


Abbildung 11.11: Original und Fake Onion Site der Suchmaschine Ahmia.fi

Schlussfolgerung: Man sollte den kryptischen Hidden Service Adressen nur vertrauen, wenn man sie aus einer vertrauenswürdigen, verifizierten Quelle bekommt. Die Ergebnislisten einer Suchmaschine für Onion Sites sind dabei nur begrenzt zuverlässig, da die Betreiber der Fake Onion Sites natürlich auch SEO-Techniken nutzen, um vor den Orginalen platziert zu werden.

11.2.4 Anonyme E-Mails mit Thunderbird

Nicht nur beim Surfen, sondern auch bei jedem Versenden und Abrufen von E-Mails werden IP-Adressen erfasst und ausgewertet. Die anhaltende Diskussion um die Vorratsdatenspeicherung zeigt, dass diese Daten bedeutsam sind. Um unbeobachtet sein E-Mail Konto nutzen zu können, ist es möglich, diese Daten mit Anonymisierungsdiensten zu verschleiern.

Vorbereitung

Es ist wenig sinnvoll, einen bisher ganz normal genutzten E-Mail Account bei einem Provider mit Vorratsdatenspeicherung plötzlich anonym zu nutzen. Es haben sich in den letzten Monaten genug Daten angesammelt, die eine Identifizierung des Nutzers ermöglichen. Der erste Schritt sollte also die Einrichtung eines neuen E-Mail Accounts sein. In der Regel erfolgt die Anmeldung im Webinterface des Providers. Für die Anmeldung ist ein Anonymiserungsdienst (JonDonym, Tor) zu nutzen. Privacy-freundliche E-Mail Provider findet man im Kapitel *Mozilla Thunderbird nutzen* oder in den Empfehlungen von TorProject.org[35].

Man kann den E-Mail Account in der Regel komplett im Webinterface des Providers nutzen. Viele Webseiten bieten jedoch keine sichere HTTPS-Verschlüsselung nach dem Stand der Technik und blockieren Tracking Features in E-Mails nicht zuverlässig. Sicherer ist die Nutzung eines E-Mail Clients. Außerdem muss man sich nicht durch ein überladenes Webinterface kämpfen, es gibt keine Probleme mit Cookies und Javascript und die OpenPGP oder S/MIME Verschlüsselung ist wesentlich einfacher und sicherer.

Thunderbird-Profil erstellen

Ich empfehle, für anonyme E-Mails Thunderbird mit einem anonymen Profil zu nutzen. Ein separates Profil gewährleistet eine konsequente Trennung von nicht-anonymer und anonymer E-Mail Kommunikation. Anderenfalls kommt man bei mehreren Konten schnell einmal durcheinander und gefährdet durch eine hektisch gesendete Mail die Anonymität des Accounts.

Man startet den Profil-Manager in der Konsole bzw. DOS-Box mit der Option -P:

```
> thunderbird -P
```

Es öffnet sich der Dialog Bild 11.12 zur Verwaltung verschiedener Profile.

[35] https://trac.torproject.org/projects/tor/wiki/doc/EmailProvider

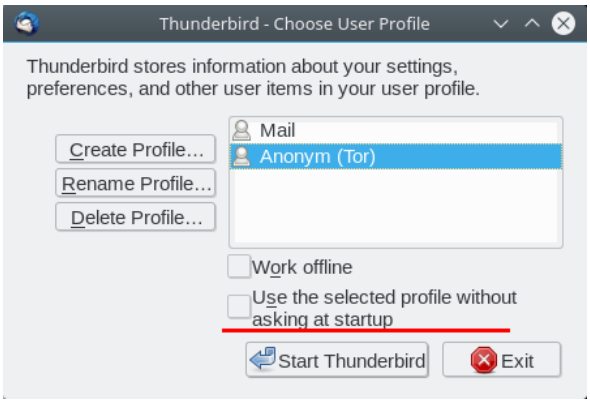


Abbildung 11.12: Profilmanager für Thunderbird

Es ist ein neues Profil zu erstellen und die Option *Beim Starten nicht nachfragen* zu deaktivieren. In Zukunft wird Thunderbird genau wie Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Thunderbird-Profil konfigurieren

Am einfachsten konfiguriert man das Profil anonym, indem man das Add-on **TorBirdy** installiert. TorBirdy kann man im Add-on Manager von Tunderbird installieren.

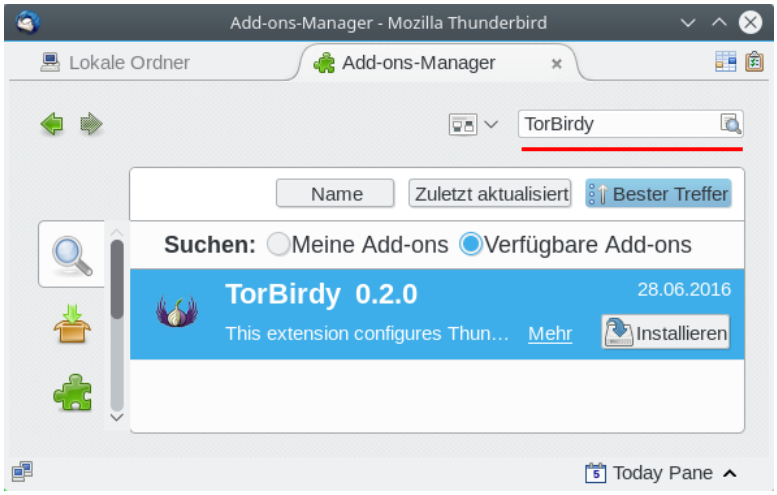
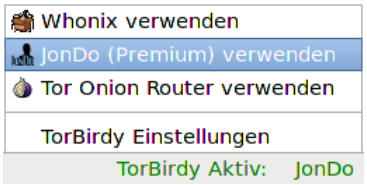


Abbildung 11.13: Add-on TorBirdy installieren

Das Add-on TorBirdy erledigt folgende Aufgaben:

- Es werden alle sicherheits- und privacy-relevanten Einstellungen aktiviert, die im Kapitel *Thunderbird nutzen* beschrieben wurden. Eine sichere und anonyme Nutzung ist ohne weitere Konfigurations gewährleistet.
- Der Assistent für die Kontenerstellung wird deaktiviert, da der Assistent aufgrund eines Fehlers unter Umständen den Proxy umgeht. Beim Anlegen eines neuen E-Mail Kontos sind POP3- und SMTP-Server per Hand zu konfigurieren. Dabei ist auf die SSL-Verschlüsselung zu achten.
- Die Proxy-Einstellung werden angepasst. Dabei kann man in der Statusleiste wählen, ob man Tor oder JonDonym (Premium) nutzen möchte.



Um Tor Onion Router zu nutzen, ist das TorBrowserBundle zu starten.

Danach kann man das Add-on Enigmail für die OpenPGP-Verschlüsselung installieren und die Wörterbücher der bevorzugten Sprachen hinzufügen.

OpenPGP Keyserver verwenden

Bei der Verwendung von *JonDo* als Proxy werden auch alle Verbindungen zu den OpenPGP Keyserver anonymisieriert, wenn man die Schlüsselverwaltung von Enigmail nutzt. Es wird dabei aber keine SSL-Verschlüsselung genutzt!

Da das TorBrowserBundle keinen HTTP-Proxy mehr enthält, sollte man mit *Tor* keine Keyserver in der Schlüsselverwaltung von Enigmail nutzen. Statt Keyserver kann man den Hidden Service http://qtt2yl5jocgrk7nu.onion mit dem TorBrowser nutzen (Hidden Service für https://keys.indymedia.org). Im Webinterface kann man nach Schlüsseln suchen oder einen eigenen Schlüssel veröffentlichen. Gefundene Schlüssel kann man mit der Maus markieren, in die Zwischenablage kopieren und dann in der Enigmail importieren.

Live-DVDs wie TAILS sind in der Regel besser konfiguriert und können auch mit *Tor* als Proxy die Keyserver anonym nutzen.

Hinweise für die Nutzung

Anonymisierungsdienste sperren den Port *25* für die Versendung von E-Mails, um nicht von Spammern missbraucht zu werden. In der Regel bieten die Provider auch den Port *465* für SSL-verschlüsselte Verbindungen oder *587* für TLS-verschlüsselte Versendung von E-Mails.

Im Dialog *Konten...* findet man in der Liste links auch die Einstellungen für den SMTP-Server. In der Liste der Server ist der zu modifizierende Server

auszuwählen und auf den Button *Bearbeiten* zu klicken. In dem sich öffnenden Dialog ist der Port entsprechend zu ändern.

TorBirdy erzwingt sicher SSL/TLS Verbindungen. Nicht alle E-Mail Provider unterstützen eine sichere SSL/TLS Verschlüsselung nach dem Stand der Technik. Probleme mit Yahoo!, Cotse und AOL sind bekannt. Diese Provider bieten keine Secure Renegotiation, was seit 2009 als schwerwiegender Bug im SSL-Protokoll bekannt ist. Wenn ständig, trotz korrekter Konfiguration, nur eine Fehlermeldung beim Senden von E-Mails erscheint, dann kann man mit der OpenSSL Bibliothek prüfen, ob eine sicher SSL-Verschlüsselung überhaupt möglich ist:

```
> openssl s_client -connect smtp.aol.com:465
...
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher : DHE-RSA-AES256-SHA
    ...
```

Sollte *Secure Renegotiation* NICHT unterstützt werden, kann man sich nur einen neuen E-Mail Provider suchen. Wenn es nicht anders geht, kann man in den Einstellungen von TorBirdy die Verbindung zu unsicheren Mailservern erlauben.

Spam-Blacklisten

Viele große E-Mail Provider sperren Tor-Nodes bei der Versendung von E-Mails via SMTP aus. Sie nutzen Spam-Blacklisten, in denen Tor-Relays häufig als "potentiell mit Bots infiziert" eingestuft sind. Wenn der E-Mail Provider eine dieser DNSBL nutzt, sieht man als Anwender von Tor nur eine Fehlermeldung beim Senden von Mails. Der Empfang funktioniert in der Regel reibungslos.

GoogleMail und Anonymisierungsdienste

GoogleMail (oder GMail) mag eine anonyme Nutzung der kostenfreien Accounts nicht. Kurz zusammengefasst kann man sagen, dass Google entweder eine IP-Adresse der Nutzer haben möchte oder die Telefonnummer. Stellungnahme des *Google account security team* zu einer Anfrage der Tor Community:

> *Hello,*
>
> *I work for Google as TL of the account security system that is blocking your access.*

Access to Google accounts via Tor (or any anonymizing proxy service) is not allowed unless you have established a track record of using those services beforehand. You have several ways to do that:

1) With Tor active, log in via the web and answer a security quiz, if any is presented. You may need to receive a code on your phone. If you don't have a phone number on the account the access may be denied.

2) Log in via the web without Tor, then activate Tor and log in again WITHOUT clearing cookies. The GAPS cookie on your browser is a large random number that acts as a second factor and will whitelist your access.

Once we see that your account has a track record of being successfully accessed via Tor the security checks are relaxed and you should be able to use TorBirdy.

Hope that helps,
Google account security team

Außerdem werden nach einem Bericht von Wired [36] zukünftig alle E-Mails der GMail Accounts in das NSA-Datacenter in Bluffdale kopiert.

11.2.5 Anonym Bloggen

Es gibt viele Gründe, um anonym zu Bloggen. Auf die möglichen Gründe möchte ich nicht weiter eingehen und mich auf einige technische Hinweise für die Umsetzung beschränken.

Die einfachste Variante:

- Man braucht einen anonymen Browser, am besten das TorBrowserBundle. Gut geeignet sind die Live-CDs TAILS und JoToSL-DVD, da diese neben einem fertig konfigurierten Browser für anonymes Surfen auch die nötigen Tools zur Anonymisierung von Bildern und Dokumenten enthalten und keine Spuren auf dem PC hinterlassen.
- Man braucht eine anonyme E-Mail Adresse, die nur in Zusammenhang mit dem Blog verwendet wird (für die Registrierung und als Kontaktadresse). Dabei ist es nicht nötig, Thunderbird als E-Mail Client zu konfigurieren. Man kann die E-Mails auch im Webinterface des Providers im Browser lesen. Dabei ist Tor zu nutzen.
- Man braucht einen Bloghoster, der anonyme Registrierung oder Registrierung mit Fake-Daten ermöglicht und anonym mit Paysafecard oder UKash bezahlt werden kann.
  - *Wordpress.com* ist empfehlenswert oder die kostenfreie Variante von *Twoday.net*. Um Premium Features bei *Wordpress.com* zu nutzen, kann man seit Nov. 2012 anonym mit Bitcoin bezahlen.[37]

[36] http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1
[37] http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/

  - Für politische Aktivitäten ist der Bloghoster *blackblogs.org* geeignet. Um ein Blog bei diesem Hoster zu eröffnen, benötigt man eine E-Mail Adresse von einem Technik Kollektiv. Auf der Policy Seite von blackblogs.org[38] findet man eine die Liste von akzeptierten E-Mail Providern. Diese E-Mail Provider bieten kostenlose Postfächer für politische Aktivisten. Um ein Postfach zu erstellen, muss man seine Gründe darlegen, aber man muss seine Identität nicht aufdecken.

- Registrierung und Verwaltung des Blogs sowie das Schreiben von Artikeln können komplett im Browser durchgeführt werden. Dabei ist stets der Anonymisierungsdienst zu nutzen. Man sollte darauf achten, dass man nicht hektisch unter Zeitdruck schnell mal einen Beitrag verfasst. Dabei können Fehler passieren, die den Autor deanonymisieren.

- Im Blog veröffentlichte Bilder und Dokumente sind stets vor dem Upload zu anonymisieren. Vor allem Bilder von Digitalkameras enthalten eine Vielzahl von Informationen, die zur Deanonymisierung führen können. Fotos von Freunden oder Bekannten sollte man nicht veröffentlichen, da durch Freundschaftsbeziehungen eine Deanonymisierung möglich ist.

- Jede Blogsoftware bietet die Möglichkeit, den Zeitpunkt der Veröffentlichung von neuen Artikeln festzulegen. Davon sollte man Gebrauch machen und neue Artikel nicht sofort veröffentlichen, sondern erst einige Stunden später freigeben, wenn man nicht online ist.

- Stilometrie (Deanonymisierung anhand des Schreibstils) ist inzwischen fester Bestandteil geheimdienstlicher Arbeit. Es ist mit (teil-) automatisierten Verfahren möglich, anonyme Texte einem Autor zuzuordnen, wenn der Kreis der Verdächtigen eingeschränkt ist und genügend Textproben der Verdächtigen vorliegen. Mit Ruhe und Konzentration beim Verfassen von Blogartikeln ist es möglich, seinen individuellen Schreibstil zu verstellen.

11.2.6 Anonymes Instant-Messaging

Verschlüsselte Chats und Instant Messaging in Kombination mit Anonymisierunsgdiensten wie Tor sind auch für potente Geheimdienste wie die NSA ein Alptraum. Es gibt keine Metadaten, starke Verschlüsselung wie OTR kann noch nicht gebrochen werden und eine Zuordnung von Traffic zu IP-Adressen wird durch die Anonymisierungsdienste verhindert.

Um Jabber/XMPP mit dem Tor Oinion Router zu anonymisieren, muss der Client folgende Anforderungen erfüllen:

1. Es muss ein SOCKS5 Proxy mit Remote DNS Resolving (ohne DNS-Leaks) konfigurierbar sein, um die Datenverkehr durch den Anonymisierungsdienst zu schicken.

2. Die Tor Hidden Service Adresse des Jabber Servers muss als *Verbindungsserver* konfigurierbar sein. Wenn Tor Onion Router genutzt wird, empfeh-

[38] https://blackblogs.org/policy/

len wir nachdrücklich die Jabber/XMPP Server, die eine Tor Hidden Service Adresse anbieten. Damit vermeidet Gefahren durch bösartige Tor Exit Nodes. Angriffe von bösartigen Tor Exit Nodes auf Jabber/XMPP wurden bereits nachgewiesen.

3. Audio- und Video-Chats mit der *libjingle* dürfen nicht verfügbar bzw. müssen deaktivierbar sein. Audio- und Video-Chats sind nicht via Anonymisierungsdienst möglich. Bei Einladung zu einem Video-Chat versucht das integrierte *Interactive Connectivity Establishment* (ICE) der *libjingle* automatisch, eine Verbindung mit oder ohne Proxy herzustellen, das ist kein Bug sondern ein Feature der ICE Spezifikation. Der User kann damit deanonymisiert werden.

4. Weitere XMPP Erweiterungen wie z.B. Jingle Dateitransfer können von einem Angreifer unter Umständen auch zur Deanonymisierung genutzt werden. Außerdem ist die Ende-zu-Ende Verschlüsselung für XMPP Erweiterungen wie Gruppenchats oder Dateitransfer in der Regel nicht oder nur eingeschränkt möglich. Idealerweise sollte ein sicherer, Torfreundlicher Jabber Client diese unsicheren Features nicht unterstützen.

11.2.7 Anonymes Instant-Messaging mit TorMessenger

Der TorMessenger wurde Ende Oktober 2015 als Beta Version freigeben. Er ist für die anonyme Nutzung von Jabber/XMPP, IRC u.ä. mit Tor Onion Router optimal vorbereitet. Aufgrund technischer Grenzen von Tor werden keine Audio- und Video-Chats unterstützt und kein Dateitransfer. Für anonyme Dateitransfers kann man OnionShare in Kombination mit dem TorBrowser-Bundle nutzen (siehe unten).

Die Installation ist ähnlich einfach, wie beim TorBrowserBundle. Download Links und Beschreibung der Installation findet man im dem Blog von TorProject.org https://blog.torproject.org. Das passende Archiv wird nach dem Downlaod entpackt - fertig. TorMessenger ist eine portable Anwendung, man kann ihn auf einem USB-Stick entpacken und damit auch problemlos in Live-DVDs wie JoToSL oder TAILS verwenden. Ein Tor Daemon ist in dem Paket enthalten und wird beim Start des TorMessengers automatisch gestartet.

Jabber Account einrichten

Beim ersten Start escheint der Assitent zum Einrichten eines Accounts. Später kann den Account Verwaltung zum Hinzufügen weiterer Accounts unter *Tools - Accounts* öffnen.

1. Im ersten Schritt wählt man das XMPP-Protokoll.

2. Im nächsten Schritt gibt man den Usernamen und die Domain ein. Wenn der Account bereit auf dem Server vorhanden ist, deaktiviert man die Option zum Erstellen des Account auf dem Server.

3. Das Passwort sollte man erst eingeben, wenn man in den Einstellungen ein Masterpasswort gesetzt hat. Anderenfalls wird das Passwort unverschlüsselt auf der Festplatte gespeichert, was der GCQH als Risiko ein-

stuft. Also bleibt das Eingabefeld für das Passwort erst einmal leer. Man kann das Passwort später beim Aufbau der Verbindung eingeben.

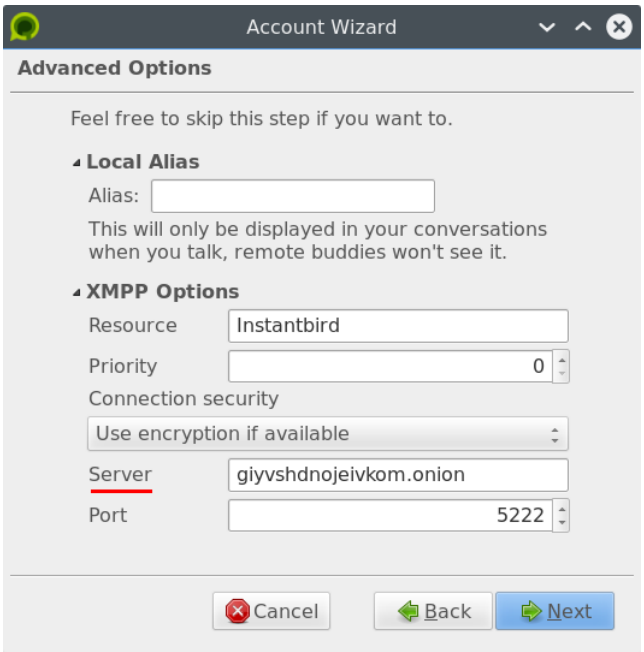


Abbildung 11.14: Tor Hidden Service Adresse in TorMessenger konfigurieren

4. Wir empfehlen ausdrücklich die Jabber/XMPP Server zu nutzen, die eine Tor Hidden Service Adresse anbieten. Damit vermeidet Gefahren durch bösartige Tor Exit Nodes. Die Hidden Service Adresse kann man als *Server* in den *XMPP Options* eintragen, wie es im Bild 11.14 zu sehen ist.

5. Abschließend wird eine Zusammenfassung angezeigt und man kann die Option zum automatischen Verbinden beim Start aktivieren.

6. Wenn man die Hidden Services der XMPP-Server nutzt, bekommt man beim ersten Aufbau der Verbindung einen Fehler. Die SSL-Zertifikate sind in der Regel nicht für die Hidden Service Adressen mit der Top-Level-Domain *.onion gültig. Man muss auf den kleinen Link *Add Exception...* unter der Fehlermeldung klicken (Bild 11.15) und das Zertifikat selbst verifizieren.

7. Zur Prüfung des SSL-Zertifikates klickt man in dem folgenden Dialog auf den Button *View* und vergleicht den Fingerprint des Zertifikates mit den Daten, die der Betreiber auf der Webseite veröffentlicht hat oder mit den Werten, die das IM-Repository für diesen Server veröffentlicht. Wenn der SHA1 bzw. SHA2 Fingerabdruck übereinstimmt, kann man die Ausnahme dauerhaft bestätigen.

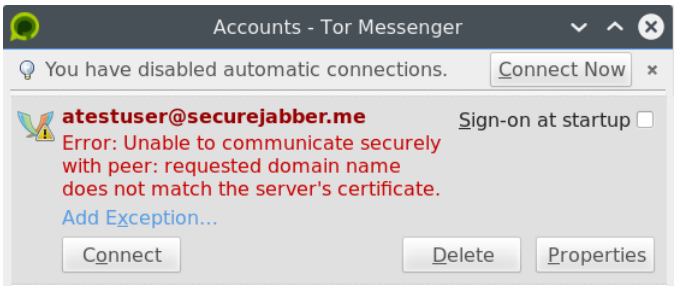


Abbildung 11.15: Fehler bei der Nutzung von Tor Hidden Services in TorMessenger

OTR-Verschlüsselung

TorMessenger unterstützt OTR für die Ende-zu-Ende Verschlüsselung. Ein Klick auf den Menüpunkt *Tools - OTR Preferences* öffnet den Dialog zur Verwaltung der OTR-Schlüssel (Bild 11.16).

Als erstes ist ein Schlüssel für den eigenen Account zu erzeugen. Wenn der Schlüssel erzeugt wurde, wird an Stelle des Buttons der Fingerabdruck angezeigt, den man veröffentlichen kann oder den Kommunikationspartnern zur Verifizierung des eigenen Schlüssels über einen unabhägigen, sicheren Kanal zur Verfügung stellen kann.

Um die OTR-Schlüssel der Kommunikationspartner anhand der Fingerprints zu verifizieren, klickt man auf den Button *View*. Ohne die Prüfung der Vertrauenswürdigkeit der Schlüssel könnte sich ein Lauscher als man-in-the-middle in die Kommunikation einschleichen. Die Software für diesen Angriff gibt es auch als Open Source, z.B. mod_otr für ejabberd.

TLS-Verschlüsselung

Die SSL/TLS-Einstellungen des TorMessengers sind etwas lax. Man kann eine bessere TLS-Verschlüsselung in den erweiterten Einstellungen erzwingen. Wenn man die Einstellungen unter *Tools - Preferences* öffnet, findet man in der Sektion *Advanced* auf dem Reiter *General* den Button für den *Config Editor*. Dort kann man folgende Werte setzen:

1. TLS 1.2 erzwingen:

   ```
   security.tls.version.min = 3
   ```

2. Alle Cipher bis auf die als sicher eingestuften Cipher deaktivieren:

   ```
   security.ssl3.ecdhe_rsa_aes_128_gcm_sha256     = true
   security.ssl3.ecdhe_ecdsa_aes_128_gcm_sha256   = true
   security.ssl3.*                                = false
   ```

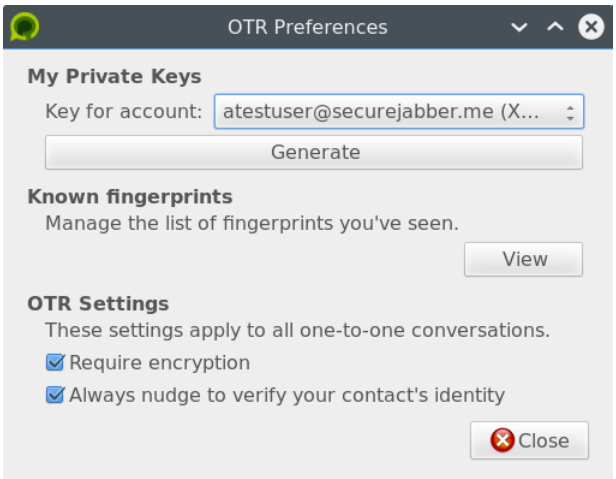


Abbildung 11.16: OTR-Schlüssel im TorMessenger verwalten

3. Insecure Renegotiation verbieten:

```
security.ssl.require_safe_negotiation            = true
security.ssl.treat_unsafe_negotiation_as_broken  = true
```

4. OCSP abschalten:

```
security.OCSP.enabled  = 0
```

5. Strenges Certifikate Pinning erwingen (z.B. für Add-on Updates):

```
security.cert_pinning.enforcement_level  = 2
```

Updates des TorMessengers

Der TorMessenger bietet den gleichen Update Mechanismus wie das TorBrowserBundle. Es wird regelmäßig geprüft, ob eine neue Version verfügbar ist, die neue Version wird via Tor herunter geladen und beim nächsten Neustart installiert. Die Einstellungen bleiben dabei erhalten.

11.2.8 Pidgin für Linux und Tor Onion Router

Pidgin für Linux erfüllt die Anforderungen leider nicht. Die *libjingle* ist in allen Distributionen leider enthalten und kann nicht deaktiviert werden. Um Pidgin mit Tor oder JonDonym zu nutzen, muss man sich selbst eine sichere Version ohne *libjingle* bauen. Für Linux Nutzer ist das ein kleines Full-Text-Adventure.

1. Bevor man mit dem Compilieren beginnen kann, müssen die Entwicklerpakete für Gtk2, GtkSpell, libXML, libidn, Mozillas NSS3 Lib, OTR und GnuPG installiert werden. Unter Debian/Ubuntu installiert man alles mit:

```
> sudo aptitude install g++ intltool libgtk2.0-dev
  libgtkspell-dev libxml2-dev libnss3-dev libidn11-dev
  libdbus-glib-1-dev libotr5-dev libgpgme11-dev
```

Optional kann man das Hardening aktivieren, um die selbst erstellten Binaries besser gegen Angriffe zu härten. Es ist das Paket *hardening-wrapper* zu installieren und vor dem üblichen Dreisatz zum Compilieren das Hardening durch Setzen einer Shellvariable zu aktivieren. Der Wrapper kümmert sich dann um die optimale Nutzung der Hardening Funktionen des Compilers und Linkers:

```
> sudo aptitude install hardening-wrapper
> export DEB_BUILD_HARDENING=1
```

Debian *wheezy* ist aufgrund der schwachen Crypto nicht mehr geeignet. Ein Update auf Debian 8 ist dringend empfohlen.

2. Wenn man SILC als verschlüsselte Alternative zu IRC nutzen möchte, dann müssen libsodium und silc-toolkit vor der Installation von Pidgin installiert werden. Nach dem Download und dem Entpacken der beiden Source Archive werden die Bibliotheken mit dem üblichen Dreisatz installiert:

```
> cd libsodium-1.0.2
> ./configure
> make
> sudo make install

> cd silc-toolkit
> ./configure
> make
> sudo make install
```

3. Den Source Code von Pidgin kann man von der Webseite des Projektes https://pidgin.im herunter laden. Nach dem Entpacken des Archives kann man eine sichere Version mit reduziertem Funktionsumfang mit folgenden Befehlen bauen:

```
> cd pidgin-2.10.11

> ./configure --disable-screensaver --disable-gstreamer
              --disable-vv --disable-meanwhile --disable-nm
              --disable-perl --disable-tcl --disable-avahi
              --enable-nss=yes --enable-gnutls=no
              --with-system-ssl-certs=/etc/ssl/certs

> make
> sudo make install
```

4. Das OTR Plug-in[39] und das OpenPGP Plug-in[40] für die Ende-zu-Ende Verschlüsselung der Kommunikation sind nicht standardmäßig in Pidgin enthalten. Man muss diese Plug-ins selbst nachinstallieren. Nach dem Download und Entpacken des Source Codes installiert man die Plug-ins wieder mit dem üblichen Dreisatz:

```
> cd pidgin-otr-4.0.1
> ./configure
> make
> sudo make install

> cd pidgin-gpg-0.9
> ./configure
> make
> sudo make install
```

5. Nach der Installation kann man Pidgin starten, die Plug-in Verwaltung öffnen, das Plug-in für die Konfiguration der NSS3 Verschlüsselung aktivieren. Die IETF empfiehlt, ausschließlich TLS 1.2 zu nutzen und stuft nur Cipher mit Forward Secrecy und AES-GCM als sicher ein:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

   Alle anderen TLS Versionen und Cipher sollte man deaktivieren, um TLS Downgrade Angriffe zu verhindern.

6. Pidgin kann eine zentrale Proxy Konfiguration für alle Accounts verwalten oder individuelle Proxy Konfigurationen für jeden Account einzeln. Um das TorBrowserBundle als Anonymisierunsgdienst zu verwenden, wählt man in der Proxy Konfiguration den Proxy-Typ *Tor/Privatsphäre*, als Host *127.0.0.1* und als Port *9150*.

7. Um Probleme mit bösartigen Tor Exit Nodes zu vermeiden, empfehlen wir die Nutzung von Jabber Servern, die als Tor Hidden Service erreichbar sind. Die Hidden Service Adresse kann man als *Verbindungsserver* auf dem Reiter *Erweitert* der Account Konfiguration eintragen.

11.2.9 Gajim (Linux) und Tor Onion Router

Gajim ist unserer Meinung nach NICHT für die Kombination mit dem Anonymisierungsdienst Tor Onion Router geeignet. Es ist eine Proxy Konfiguration für Tor vorbereitet, aber Gajim enthält Bugs, welche die Anonymität und Sicherheit bei der Verwendung von Tor gefährden.

[39] http://www.cypherpunks.ca/otr/
[40] https://github.com/segler-alex/Pidgin-GPG/wiki/Downloads

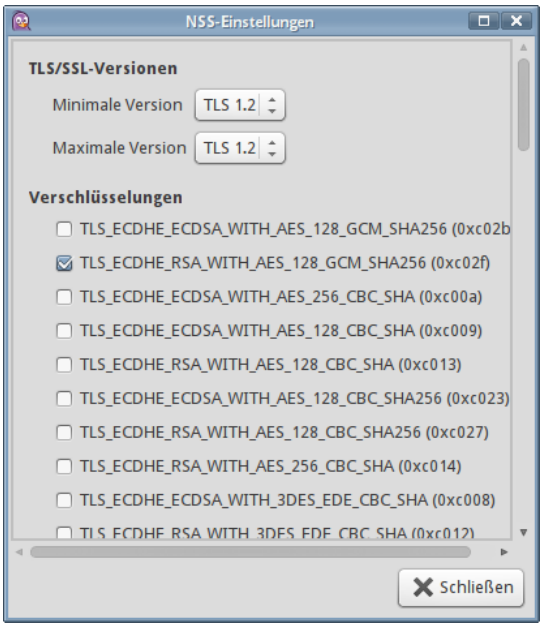


Abbildung 11.17: TLS Cipher für Pidgin konfigurieren

Wir haben Gajim 0.16.5 unter Ubuntu 16.04 kurz getestet (Stand: Nov. 2016). Gajim für Windows verhält sich möglicherweise etwas anders. Evtl. ist die *libjingle* nicht enthalten? Vielleicht kann man sich ähnlich wie bei Pidgin einen Tor-safe Gajim für Linux selbst bauen?

DNS-Leaks: Gajim überlässt die Auflösung von Hostnamen in IP-Adressen nicht dem SOCKS5 Proxy, sondern macht es selbst und umgeht dabei die Proxy Einstellungen. Diese DNS-Leaks sind ein Security Bug und können die Anonymität gefährden. Im TorProject Wiki findet man folgende Empfehlung, das Problem zu umgehen:

> *To prevent this you have to take the hostname of your jabber-server you want to connect to and resolve its IP,e.g. with tor-resolve and paste the IP adress into Account -> Connection -> Custom Hostname and Port. Now you're safe (probably)*

Vor einigen Jahren war diese Empfehlung vielleicht ok, die IP-Adresse (oder die Tor Hidden Service Adressen) des XMPP Servers als Verbindungsserver einzutragen. Neumodisch aufgemotzte Jabber Server bieten aber mehrere Services unter unterschiedlichen Hostnamen. Wenn man mit dem Account verbunden ist, kann man sie unter *Aktionen - Dienste durchsuchen* abrufen. Der Jabber Server von conversations.im bietet z.B. die in Abbildung 11.18 zu sehenden Dienste.

Man müsste also auch die IP-Adressen der Services *conference.conversations.im*, *proxy.conversations.im* usw. ermitteln und lokal auf dem Rechner fest vorgeben, um DNS-Leaks für diese Hostnamen

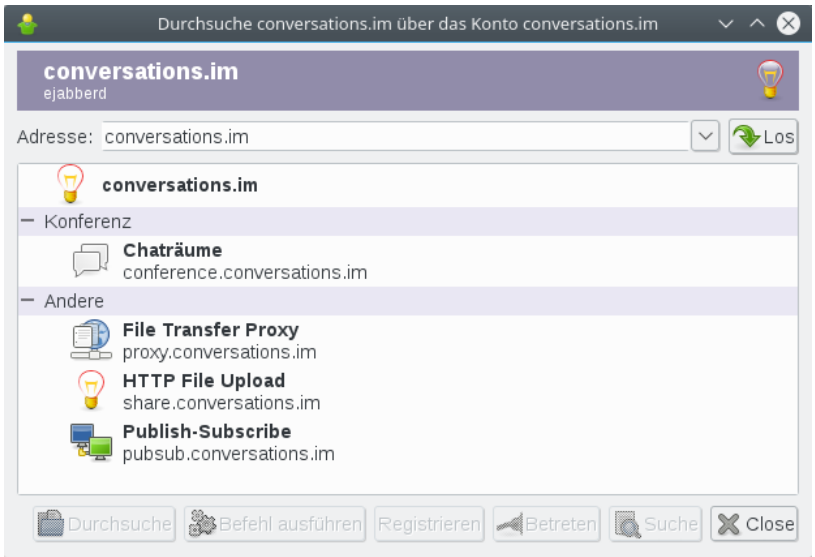


Abbildung 11.18: Services von conversations.im

ebenfalls zu vermeiden (könnte man unter Linux in */etc/hosts* machen). Aber die Services können sich jederzeit ändern, der Admin könnte neue Services hinzugefügt und automatisch an die Clients verteilen... Man müsste es ständig beobachten und bei Bedarf anpassen. Unsicher.

Außerdem treten DNS-Leaks auf, wenn bei einem Dateitransfer ein Dateitransfer Proxy genutzt wird, der vom Kommunikationspartner angeboten wird. Die Nutzung von Dateitransfer Proxies könnte man in der Account Konfiguration komplett deaktivieren.

ICE: Gajim für Linux enthält eine Implementierung der *libjingle* für Audio- und Videochats. Wenn ein Angreifer eine Einladung zu einem Audio Chat schickt, dann versucht das *Interactive Connectivity Establishment* (ICE) der libjingle auf unterschiedlichen Wegen, irgendwie eine Verbindung für einen Audio Channel herzustellen und umgeht dabei auch die Proxy Einstellungen. **Auch wenn man Tor als Proxy konfiguriert hat, versucht ICE mit oder ohne Tor irgendwie die Verbindung zum Angreifer herzustellen. Das kann den Nutzer deanonymisieren.** (Dieses Verhalten ist kein Bug sondern ein Feature, dass in der Spezifikation so vorgeschrieben ist).

Ein Beispiel: Unter anderem schickt Gajim eine SSDP Discovery Message ins LAN, um einen UPnP-fähigen Router zu finden, der die externe IP-Adresse liefern könnte:

```
M-SEARCH * HTTP/1.1
Host: 239.255.255.250:1900
Man: "ssdp:discover"
```

```
ST: urn:schemas-upnp-org:service:WANIPConnection:1
MX: 3
User-Agent: gajim GSSDP/0.14.14
```

Wenn der Angreifer innerhalb des gleichen lokalen Netz sitzt (innerhalb des Firmennetzwerk, bei Starbucks o.ä.), dann hat man damit verloren. Wenn der Angreifer diese SSDP Discovery Message unmittelbar als nach einer Einladung zu einem Audio Chat sieht, dann weiß er, an welchem Rechner das anonyme Gegenüber sitzt.

Wenn Gajim zufällig einen UPnP-fähigen Router findet, dann ist man auch gegenüber einem Angreifer aus dem Internet deanonymisiert. Bei vielen Heimroutern ist UPnP standardmäßig aktiviert, um die Usability zu verbessern.

Unser Test ist nicht gründlich und ist nicht abschließend. Wir haben ein bisschen rumgespielt und mit Wireshark den Datenverkehr beobachtet, das ist kein Security Audit! Insbesondere haben wir keine Zeit gehabt, wirklich im Code nachzuschauen. Wir haben genug Probleme gefunden, um vor der Kombination Gajim+Tor zu warnen.

11.2.10 Anonymes Instant-Messaging mit TorChat

TorChat ist ein Instant-Messaging Client mit einem genialen Konzept. Jeder Account ist ein Tor Hidden Service. Die Kommunikation erfolgt direkt zwischen den Beteiligten, es gibt keinen Serverdienst wie bei Jabber (XMPP) oder anderen Instant-Messaging Varianten. Die Verschlüsselung wird durch Tor sichergestellt. Außerdem kann ein externer Beobachter nicht erkennen, welche Art der Kommunikation abläuft.

Die Projektwebseite https://github.com/prof7bit/TorChat/downloads stellt Installationspakete für Windows und Debian basierte Linux Distributionen zum Download bereit. Außerdem kann man die Sourcen nutzen.

Windows: Das ZIP-Archiv ist nach dem Download zu entpacken - fertig. Im Verzeichnis *bin* findet man die Datei *torchat.exe*. Ein Doppelklick auf die Datei startet alles Nötige. Zur Vereinfachung des Starts kann man eine Verknüpfung erstellen und auf den Desktop ziehen.

Debian, Ubuntu, Mint: TorChat ist in Repositories enthalten. Man kann es mit dem bevorzugten Paketmanager installieren:

```
> sudo apt install torchat
```

Sourcen: Für alle Nicht-Debian Linuxe und UNIXe kann man das Source-Paket nutzen. Auch hier benötigt man *Tor, Python-2.x* sowie *WxGTK für Python*. Nach der Installation der nötigten Bibliotheken und dem Entpacken der Sourcen startet man TorChat in dem *src*-Verzeichnis:

```
> python torchat.py
```

Beim Start von TorChat wird eine Instanz von Tor mit den passenden Parametern gestartet. Ein Account wird automatisch erstellt, wenn noch nicht vorhanden. Dann dauert es 15-20 min bis der Account bekannt wird.

Die Bedienung ist einfach. Man klickt mit der rechten Maustaste in das Hauptfenster und fügt eine TorChat-ID hinzu. Wenn das Symbol farbig dargestellt wird, kann man eine Nachricht schreiben oder eine Datei senden. Farblos dargestellt Accounts sind nicht online. Eine TorChat-ID ist eine kryptische Tor Hidden Service Adresse ohne die Endung *.onion*.

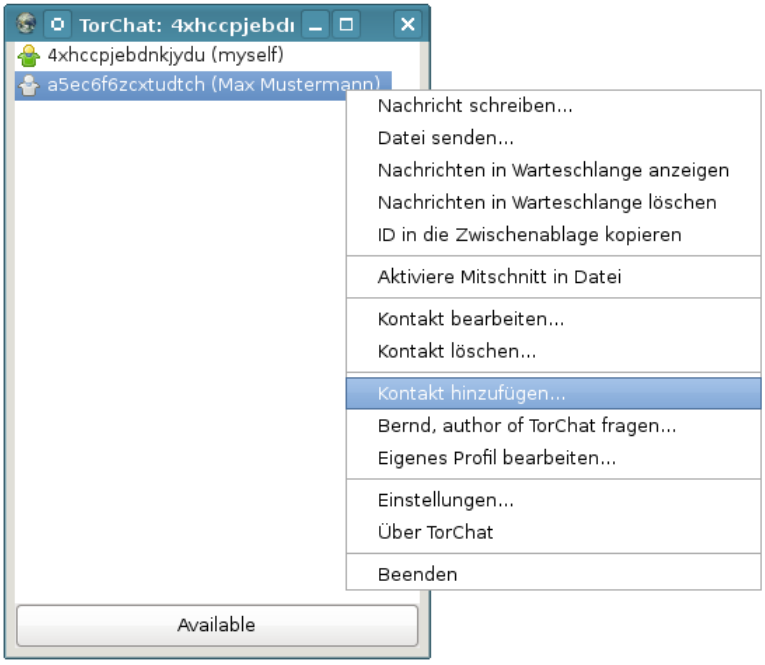


Abbildung 11.19: TorChat Hauptfenster

WICHTIG: TorChat ist immer über den Menüpunkt *Beenden* zu schließen. Nur dann wird auch die gestartete Instanz von Tor sauber beendet.

Security Hinweis für TorChat

Eine Security Analyse[41] der Universität Tallin von 2015 zeigt zahlreiche Schwächen in TorChat auf:

- Denial-of-Service Angriffe auf einen bekannten Account sind möglich

[41] http://kodu.ut.ee/ arnis/torchat_thesis.pdf

- versteckstes Monitoring der Online-Zeiten eines bekannten Account ist möglich, indem man eine Kontaktanfrage sendet, die automatisch ohne Bestätigung durch den Empfänger übernommen wird
- durch die Verwendung eines kryptografisch schwachen Zufallsgenerators ist es einem Angreifer möglich, die Identität der Kommunikationspartners eines bekannten Accounts bei der Kontaktaufnahme zu übernehmen und im Namen dieser Identitäten Nachrichten zu senden sowie Dateitransfers einzuleiten

Die Analyse kommt zu dem Schluss, das TorChat nur unter der Bedingung sicher verwendet werden kann, wenn die TorChat-ID dem Angreifer nicht bekannt ist. **Die eigene TorChat-ID ist also geheim zu halten** und nur ausgewählten Personen zur Verfügung zu stellen.

11.2.11 Anonymes Instant-Messaging mit Ricochet

Ricochet ist eine Weiterentwicklung von TorChat. Derzeit ist Ricochet noch im Alpha Stadium. Der Instant Messenger verwendet ebenfalls die Technik der Tor Hidden Services, um eine sichere und anonyme Kommunikation zu ermöglichen.

Zukünftig soll OTR Verschlüsselung als zusätzlicher Security Layer integriert werden, da sich die Geheimdienste um eine Entschlüsselung des Tor Traffics bemühen. Bisher ist nur anonymer Chat möglich, kein Dateitransfer. Für anonyme Dateitransfers kann man OnionShare in Kombination mit dem TorBrowserBundle nutzen (siehe unten).

Die Installation ist etwas einfacher als bei TorChat. Von der Projektseite https://ricochet.im/ kann man Archive für Windows, MacOS oder Linux herunter laden. Das Archiv ist zu entpacken und das Programm textitricochet in dem neu erstellten Verzeichnis aufzurufen. Im Terminal funktioniert es mit:

```
> cd ricochet
> ./ricochet
```

Ein Tor Daemon wird dabei automatisch im Hintergrund gestartet. Zur Vereinfachung kann man sich einen Programm Starter auf dem Desktop erstellen oder ins Programm Menü integrieren. Anleitungen liefert die Hilfe des verwendeten Betriebssystems.

Als erste Aktion kann man die Verbindung zum Tor Netzwerk konfigurieren, wenn man Probleme aufgrund restriktiver Firewalls hat. Dann wählt man *Connect*, um den Tor Deamon zu starten. Es dauert einige Minuten, bis man für die Kommunikationspartner erreichbar ist.

Das Chatfenter ist einfach augebaut. Man kann Kontakte hinzufügen (+) und einige Optionen zur Konfiguration anpassen. Die Nachricht (Message) wird beim Klicken von *Add* als *contact request* an den gewünschten Kommunikationspartner gesendet. Damit erleichtert man dem Gegenüber die

Aufnahme der eigenen Adresse in die Kontaktliste.

Im Dialog zum Hinzufügen von Kontakten findet man auch die eigene Adresse (oben, im Bild 11.20), die man kopieren und veröffentlichen bzw. anderen Kommunikationspartnern über einen sicheren Kanal zur Verfügung stellen kann.

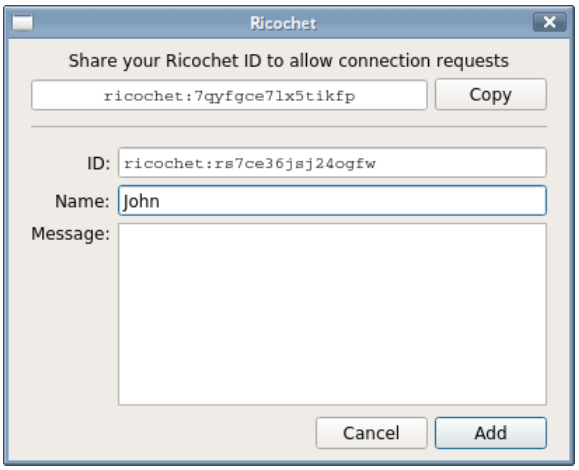


Abbildung 11.20: Ricochet (Kontakt hinzufügen und eigene Adresse auslesen)

11.2.12 Dateien anonym tauschen via Tor

OnionShare[42] ist ein kleines Tool, um in Kombination mit dem TorBrowser-Bundle Dateien zu tauschen. Es ist eine ideale Ergänzung zu TorMessenger oder Ricochet, denen die Möglichkeit zum Tauschen von Dateien (noch) fehlt.

1. Der Absender benötigt OnionShare und den Tor Daemon des TorBrowserBundles, um die Dateien zum Download bereitzustellen. OnionShare stellt einen Tor Hidden Service bereit, unter dem die Dateien abgerufen werden können.

2. Der oder die Empfänger benötigen nur den TorBrowser, um die bereitgestellten Dateien herunter zu laden. Den Link zum Download bekommen die Empfänger über einen anderen sicheren Kanal, z.B. via TorMessenger oder Ricochet.

Installation von OnionShare:

- Für Windows und MacOS stehen auf der Download Website Setup Dateien zur Installation bereit.

- Für Unbuntu gint es ein PPA-Repository, dass man mit folgenden Kommandos zur Installation nutzen kann:

[42] https://onionshare.org

```
sudo add-apt-repository ppa:micahflee/ppa
sudo apt update
sudo apt install onionshare
```

- Für alle anderen Linux Distributionen muss man OnionShare selbst compilieren. Eine Anleitung findet man auf der Webseite.

Nach dem Start von OnionShare kann man im Hauptfenter Dateien zur Liste der gesharten Dateien hinzufügen und den Service starten. Der Tor Daemon des TorBrowserBundle wird genutzt, um den Hidden Service bereitzustellen, das TorBrowserBundle muss also gestartet werden, bevor man die Dateien zum Download freigeben kann.

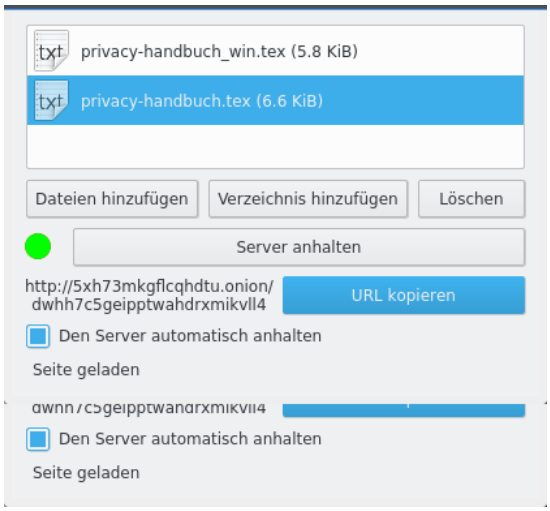


Abbildung 11.21: OnionShare Hauptfenster

Wenn die Option *Den Server automatisch anhalten* aktiviert, dann wird der Tor Hidden Service nach dem ersten erfolgreichen Download sofort wieder beendet. Das ist ein Sicherheitsfeature, da es im Tor Netz auch bösartige Nodes gibt, die neue Tor Hidden Services testen und teilweise auch angreifen.[43]

Wenn der Service erfolgreich gestartet ist, kann man die Tor Onion URL in die Zwischenablage kopieren und an den oder die Empfänger schicken, am besten via Instant Messenger. Der oder die Empfänger können die Adresse dann im TorBrowser aufrufen und die bereitgestellten Dateien als ZIP-Archiv herunter laden.

1-Click-Hoster

1-Click-Hoster sind eine weitere mögliche Alternative. Mit dem TorBrowser-Bundle kann man anonym Datieen bei einem 1-Click-Hoster hochladen und den Download-Link veteilen.

[43] https://www.schneier.com/blog/archives/2016/07/researchers_dis.html

- Auf diesen Hostern sind die Uploads nur eine begrenzte Zeit verfügbar (1-4 Wochen):
  - http://www.senduit.com
  - http://www.wikisend.com (Passwortschutz möglich)
  - http://www.turboupload.com (Löschen der Uploads möglich)
  - http://www.filefactory.com (benötigt Javascript)
  - http://www.share-now.net
- Für Langzeit-Hosting kann man folgende Dienste verwenden:
  - http://www.mediafire.com (Registrierung für Uploads nötig)
  - http://ompldr.org (benötigt Cookies für Uploads)

BitTorrent über einen Anonymisierungsdienst ???

Die naheliegende Variante ist es, BitTorrent über einen Anonymisierungsdienst wie Tor zu nutzen, um die eigene IP-Adresse zu verstecken. Das funktioniert nur begrenzt. Das BitTorrent-Protokoll überträgt die IP-Adresse des Clients auch im Header der Daten und es ist relativ einfach möglich, die Teilnehmer zu deanonymiseren. Im Moment hat die Abmahn-Industrie den Weg noch nicht gefunden. Im Blog von TorProjekt.org findet man eine ausführliche Erläuterung, warum BitTorrent via Tor NICHT anonym ist [44].

Anonyme Peer-2-Peer Netze

Einige Projekte für anonymes, unbeobachtetes Filesharing:

- **I2P Snark:** Das Invisible Internet Project bietet anonymes Filesharing innerhalb des Netzes. Eine kurze Einführung findet man im Kapitel zum Invisible Internet.
- **GNUnet:** bietet anonymes, zensurresistentes Filesharing ohne zentrale Server. Alle Teilnehmer leiten Daten für andere Teilnehmer weiter und stellen selbst Dateien bereit. Da weitergeleitete Daten nicht von Daten unterscheidbar sind, die von einem Teilnehmer selbst stammen, ergibt sich eine hohe Anonymität. Es ist ein echtes GNU-Projekt (bitte nicht mit Gnutella verwechseln). Weitere Informationen auf der Projektwebsite http://gnunet.org.

11.2.13 Tor Bad Exit Nodes

Ein sogenannter *Bad-Exit-Node* im Tor-Netz versucht den Traffic zu beschnüffeln oder zusätzliche Inhalte in eine (nicht SSL-gesicherte) Website einzuschmuggeln. Bedingt durch das Prinzip des Onion Routings holt der letzte Node einer Kette die gewünschten Inhalte. Diese Inhalte liegen dem Node im Klartext vor, wenn sie nicht SSL- oder TLS-verschlüsselt wurden.

[44] https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Durch einfaches Beschnüffeln wird die Anonymität des Nutzers nicht zwangsläufig kompromittiert, es werden meist Inhalte mitgelesen, die im Web schon verfügbar sind. Erst wenn Login-Daten unverschlüsselt übertragen werden oder man-in-the-middle Angriffe erfolgreich sind, können die Bad Exit Nodes an persönliche Informationen gelangen. Persönliche Daten, bspw. Login Daten für einen Mail- oder Bank-Account, sollten nur über SSL- oder TLS-gesicherte Verbindungen übertragen werden. Bei SSL-Fehlern sollte die Verbindung abgebrochen werden. Das gilt für anonymes Surfen via Tor genauso, wie im normalen Web.

Einige Beispiele für Bad Exits:

1. Die folgenden Nodes wurde dabei erwischt, den Exit Traffic zu modifizieren und Javascript in abgerufene Websites einzuschmuggeln. Dabei handelte es sich zumeist um Werbung oder Redirects auf andere Seiten.

apple	$232986CD960556CD8053CBEC47C189082B34EF09
CorryL	$3163a22dc3849042f2416a785eaeebfeea10cc48
tortila	$acc9d3a6f5ffcda67ff96efc579a001339422687
whistlersmother	$e413c4ed688de25a4b69edf9be743f88a2d083be
BlueMoon	$d51cf2e4e65fd58f2381c53ce3df67795df86fca
TRHCourtney1..10	$F7D6E31D8AF52FA0E7BB330BB5BBA15F30BC8D48
	$AA254D3E276178DB8D955AD93602097AD802B986
	$F650611B117B575E0CF55B5EFBB065B170CBE0F1
	$ECA7112A29A0880392689A4A1B890E8692890E62
	$47AB3A1C3A262C3FE8D745BBF95E79D1C7C6DE77
	$0F07C4FFE25673EF6C94C1B11E88F138793FEA56
	$0FE669B59C602C37D874CF74AFEA42E3AA8B62C6
	$E0C518A71F4ED5AEE92E980256CD2FAB4D9EEC59
	$77DF35BBCDC2CD7DB17026FB60724A83A5D05827
	$BC75DFAC9E807FE9B0A43B8D11F46DB97964AC11
Unnamed	$05842ce44d5d12cc9d9598f5583b12537dd7158a
	$f36a9830dcf35944b8abb235da29a9bbded541bc
	$9ee320d0844b6563bef4ae7f715fe633f5ffdba5
	$c59538ea8a4c053b82746a3920aa4f1916865756
	$0326d8412f874256536730e15f9bbda54c93738d
	$86b73eef87f3bf6e02193c6f502d68db7cd58128

   Diese Tor-Nodes sind nicht mehr online, die Liste ist nur ein Beispiel.

2. Die folgenden Nodes wurden bei dem Versuch erwischt, SSL-Zertifikate zu fälschen, um den verschlüsselten Traffic mitlesen zu können:

   (a) *LateNightZ* war ein deutscher Tor Node, der 2007 beim man-in-the-middle Anriff auf die SSL-Verschlüsselung erwischt wurde.[45]

   (b) *ling* war ein chinesischer Tor Node, der im Frühjahr 2008 versuchte, mit gefälschten SSL-Zertifikaten die Daten von Nutzern zu ermitteln. Gleichzeitig wurde in China eine modifizierte Version von Tor

[45] http://www.teamfurry.com/wordpress/2007/11/20/tor-exit-node-doing-mitm-attacks/

in Umlauf gebracht, die bevorzugt diesen Node nutzte. Die zeitliche Korrelation mit den Unruhen in Tibet ist sicher kein Zufall [46].

(c) Im Sept. 2012 wurden zwei russische Tor Nodes mit den IP-Adressen 46.30.42.153 und 46.30.42.154 beim SSL man-in-the-middle Angriff erwischt.

(d) Im April 2013 wurde der russische Tor Node mit der IP-Adresse 176.99.10.92 beim SSL man-in-the-middle Angriff auf Wikipedia und auf IMAPS erwischt [47].

Beide Tor Nodes gingen kurz nach ihrer Entdeckung offline. Inzwischen können die Geheimdienste durch Zusammenarbeit mit kompromittierten Certification Authorithies gültige SSL-Zertifikate fälschen. Diese man-in-the-middle Angriffe sind sehr schwer erkennbar.

3. Im Februar/März 2012 haben mehrere Exit-Nodes in einer konzertierten Aktion die HTTPS-Links in Webseiten durch HTTP-Links ersetzt. Wie man damit erfolgreich die SSL-Verschlüsselung ausgehebeln kann, wurde auf der Black Hack 2009 beschrieben. Die Software für diesen Angriff heisst *ssl-stripe* und ist als Open Source verfügbar.

```
Bradiex            bcc93397b50c1ac75c94452954a5bcda01f47215
                   IP: 89.208.192.83
TorRelay3A2FL      ee25656d71db9a82c8efd8c4a99ddbec89f24a67
                   IP: 92.48.93.237
lolling            1f9803d6ade967718912622ac876feef1088cfaa
                   IP: 178.76.250.194
Unnamed            486efad8aef3360c07877dbe7ba96bf22d304256
                   IP: 219.90.126.61
ididedittheconfig  0450b15ffac9e310ab2a222adecfef35f4a65c23
                   IP: 94.185.81.130
UnFilTerD          ffd2075cc29852c322e1984555cddfbc6fb1ee80
                   IP: 82.95.57.4
```

4. Im Oktober 2014 wurde ein Tor Exit Node aufgespürt, der Windows Binaries (z.B. DLLs oder EXE-Dateien) beim Download on-the-fly mit dem Trojaner OnionDuke infizierte, einer Variation der russischen Cyberwaffe MiniDuke. Der Trojaner sammelte Login Daten und spionierte die Netzwerkstruktur der Opfer aus. F-Secure konnten die ersten Infektionen mit OnionDuke auf Oktober 2013 datieren. Der Bad Exit Node wurde nur gefunden, weil ein Sicherheitsforscher gezielt nach diesem Angriff suchte.[48]

5. Im April 2015 wurden 70 Bad Tor Nodes identifiziert, die den Hidden E-Mail Service angegriffen hatten. Die Betreiber von SIGAINT warnen, dass es den Angreifern gelungen ist, den Hidden Service mit einem man-in-the-middle Angriff zu kompromittieren und möglicherweise Daten inklusive Login Credentials mitzulesen.[49]

[46] http://archives.seul.org/or/talk/Mar-2008/msg00213.html
[47] https://trac.torproject.org/projects/tor/ticket/8657
[48] http://heise.de/-2457271
[49] https://lists.torproject.org/pipermail/tor-talk/2015-April/037549.html

> *I think we are being targeted by some agency here. That's a lot of exit nodes.* SIGAINT Admin

Diese 70 Tor Nodes meldeten sich innerhalb eines Monats kurz vor dem Angriff als neue Tor Nodes im Netzwerk an. 31 weitere Nodes stehen noch in dem Verdacht, ebenfalls zu dieser Gruppe zu gehören, aber noch nicht aktiv angegriffen zu haben.

6. Um passiv schnüffelnde Tor Exit Nodes in eine Falle tappen zu lassen, hat Chloe im Juni 2015 einen Honigtopf aufgestellt und 11 passiv schnüffelnde Exit Nodes aufgespürt. Zwei der elf Nodes hatten Guard Status.[50]

7. Im März 2016 haben 14 Bad Exit Nodes in einer konzertierten Aktion versucht, sich als man-in-the-middle in STARTTLS Verschlüsselung einiger Jabber/XMPP Server einzuschleichen.[51]

   Folgende Jabber Server waren von dem Angriff betroffen:

   - freifunk.im
   - jabber.ccc.de
   - jabber.systemli.org
   - jappix.org
   - jodo.im
   - pad7.de
   - swissjabber.ch
   - tigase.me

8. Tor Exit Nodes aus dem Iran sind generell als Bad Exits markiert. Diese Nodes unterliegen der iranischen Zensur. Außerdem wird beim Aufruf von Webseiten über diese Nodes von der staatlichen Firewall ein unsichtbarer IFrame aus dem Hidden Internet[52] of Iran eingefügt.

```
<iframe src="http://10.10.34.34" style="width: 100%;
   height: 100%" scrolling="no" marginwidth="0"
   marginheight="0" frameborder="0" vspace="0" hspace="0">
</iframe>
```

9. Die Unterlagen des Whistleblowers E. Snowden haben bestätigt, dass NSA und GCHQ passiv schnüffelnde Exit-Nodes betreiben. Die NSA soll damals 10-12 leistungsfähige Tor-Server genutzt haben (aktuelle Angriffe zeigen, dass es inzwischen deutlich mehr sein müssen). Zum Engagement des GSHQ wurden keine Zahlen bekannt.

10. Europol betreibt seit Jahren ein Projekt mit dem Ziel *to provide operational intelligence related to TOR*. Die Formulierung lässt vermuten, dass ebenfalls passiv schnüffelnde Exit-Nodes genutzt werden.

[50] https://chloe.re/2015/06/20/a-month-with-badonions/
[51] https://tech.immerda.ch/2016/03/xmpp-man-in-the-middle-via-tor/
[52] http://arxiv.org/abs/1209.6398

11.2.14 Tor Good Exit Nodes

Im Abschnitt *Tor Bad Exits* sind einige Nodes genannt, denen man nicht trauen sollte. Diese Aufzählung kann nicht abschleißend und vollständig sein.

Verschiedene Sicherheitsforscher haben nachgewiesen, dass es recht einfach möglich ist, mit schnüffelnden Exits Informationen über die Nutzer zu sammeln (D. Egerstad 2007, C. Castelluccia 2010...). Man kann davon ausgehen, dass es verschiedene Organisationen gibt, die mit unterschiedlichen Interessen im Tor Netz nach Informationen phishen. Auch SSL-verschlüsselte Verbindungen sind nicht 100% geschützt. C. Soghoian und S. Stamm haben in einer wiss. Arbeit gezeigt, dass Geheimdienste wahrscheinlich in der Lage sind, gültige SSL-Zertifikate zu faken.

Als Verteidigung können Nutzer in der Tor-Konfiguration Exit Nodes angeben, denen sie vertrauen und ausschließlich diese Nodes als Exit-Nodes nutzen. Welche Nodes vertrauenswürdig sind, muss jeder Nutzer selbst entscheiden, wir können nur eine kurze Liste als Anregung zum Nachdenken liefern.

- Torservers.net ist eine vertrauenswürdige Organisation, die mehrere Exit-Nodes betreibt.
- Die von der Swiss Privacy Foundation betriebenen Server sammeln keine Informationen. Eine Liste der Server findet man unter: https://www.privacyfoundation.ch/de/service/server.html.
- Der CCC betreibt zur Zeit acht Tor Nodes (siehe Liste im TorAtlas unter https://atlas.torproject.org/#search/chaoscomputerclub).
- Der Tor Node *Digitalcourage3ip1* wird vom Verein Digitalcourage e.V. betrieben (vormals FoeBuD).[53]
- Die Heinlein Support GmbH betreibt den Tor Node *mailboxorg* und empfiehlt die Konfiguration von MapAdresses in der torrc, so dass dieser Node als Exit Node für alle Mailbox.org Dienste genutzt wird.
- .... bitte selbst die Liste erweitern

Bei der Auswahl der Server sollte man nicht einfach nach dem Namen im TorStatus gehen. Jeder Admin kann seinem Server einen beliebigen Namen geben und den Anschein einer vertrauenswürdigen Organisation erwecken. Die Identität des Betreibers sollte verifiziert werden, beispielsweise durch Veröffentlichung auf einer Website.

Konfiguration in der torrc

In der Tor Konfigurationsdatei */etc/tor/torrc* bzw. für das TorBrowserBundle in *<TorBrowserBundleVerzeichnis>/Browser/TorBrowser/Data/Tor/torrc* kann man die gewünschten Nodes mit folgenden Optionen konfigurieren:

[53] https://digitalcourage.de/support/tor

```
StrictExitNodes 1
ExitNodes $9BDF3EEA1D33AA58A2EEA9E6CA58FB8A667288FC,
          $1A1DA6B9F262699A87F9A4F24EF48B50148EB018,
          $31A993F413D01E68117F76247E4F242095190B87,
          $A07FF746D9BA56C3F916BBD404307396BFA862E0,
          $A3279B1AC705C9F3478947598CF0557B81E12DE1,
          $AB176BD65735A99DCCB7889184E62EF0B2E35751,
          $B7BE1D35762155FEB2BC9DAE0A157C706D738FE5,
          $85D4088148B1A6954C9BFFFCA010E85E0AA88FF0,
          $39659458160887CC8A46FAE627EE01EEDAAED07F,
          $0111BA9B604669E636FFD5B503F382A4B7AD6E80,
          $AD86CD1A49573D52A7B6F4A35750F161AAD89C88,
          $DC41244B158D1420C98C66F7B5E569C09DCE98FE,
          $B060482C784788B8A564DECD904E14CB305C8B38,
          $88487BDD980BF6E72092EE690E8C51C0AA4A538C,
          $95DA61AEF23A6C851028C1AA88AD8593F659E60F,
          $95DA61AEF23A6C851028C1AA88AD8593F659E60F,
          $487092BA36F4675F2312AA09AC0393D85DAD6145
```

Die erste Option gibt an, dass nur die im folgenden gelisteten Nodes als Exit verwendet werden dürfen. Für die Liste der Exits nutzt man die Fingerprints der Nodes, beginnend mit einem Dollar-Zeichen. Die Fingerprints erhält man von verschiedenen TorStatus Seiten. Diese Liste enthält die oben genannten Nodes.

11.3 Finger weg von unseriösen Angeboten

Neben Projekten, die sich wirklich um eine anonyme Lösung für Surfer bemühen, gibt es immer wieder Angebote, die unbedarfte Anwender ködern wollen.

11.3.1 Tor-Boxen

Sogenannte Tor-Boxen wie Anonabox oder SafePlug leiten als Router den gesamten Traffic eines Computers oder Heimnetzwerkes oder als Proxy nur den HTTP-Traffic durch Tor. Die Anbieter versprechen eine einfachste Installation und gleichzeitig die Anonymtät des Tor-Netzwerkes. Aber manchmal ist *Einfach* das Gegenteil von *Anonym*.

Anonymes Surfen erfordert in erster Linie eine sichere Browserkonfiguration. Wer mit einem beliebigen Browser (z.B. Internet Explorer, Google Chrome oder Safarie) ohne privacy-freundliche Konfiguration im Internet surft, der kann sich die Nutzung von Tor sparen, damit surft man nicht anonym. Die einzige, von den Tor-Entwicklern empfohlene Variante zum anonymen Surfen ist die Nutzung des TorBrowserBundle.

> *The most crucial problem with a torifying proxy is that it uses a bring-your-own-browser system, as opposed to a hardened browser, and therefore is susceptible to browser-based privacy leaks. This is why it's better to use the Tor Browser Bundle.* (Quelle: Blog TorProject.org)

11.3.2 Web-Proxys

Web-Proxys mit HTTPS-Verschlüsselung sind ein probates Mittel, um Zensur im Internet zu umgehen. Sie sind aber als Anonymisierungsdienste unbrauchbar. Mit kruden HTML-Elementen oder Javascript ist es möglich, die meisten Web-Proxys auszutricksen und die reale IP-Adresse des Nutzers zu ermitteln.

Die folgende Tabelle zeigt eine Liste bekannter Webproxys, die den Anonymitätstest der JonDos GmbH nicht bestehen:

Betreiber	HTML/CSS	Javascript	Java
Anonymouse	gebrochen	gebrochen	gebrochen
Cyberghost Web		gebrochen	gebrochen
Hide My Ass!		gebrochen	gebrochen
WebProxy.ca		gebrochen	gebrochen
KProxy		gebrochen	gebrochen
Guardster		gebrochen	gebrochen
Megaproxy	gebrochen	nicht verfügbar	nicht verfügbar
Proxify		gebrochen	gebrochen
Ebumna	gebrochen	gebrochen	gebrochen

Einige Webproxys erlauben es, Javascript mit dem Aktivieren einer Option auf der Startseite zu blockieren. Es ist zwingend notwendig, diese Option zu aktivieren, da alle Webproxys mit Javascript ausgetrickst werden können! Außerdem sollte man Javascript im Browser deaktivieren, damit keine Scripte in Bildern, Werbebannern o.ä. durch den Proxy geschmuggelt werden können.

CTunnel.com

CTunnel.com ist ein ganz besonderer Web-Proxy, der hier etwas ausführlicher behandelt werden soll. Man verspricht zwar eine anonyme Nutzung des Internet. Die Entwickler haben sich aber große Mühe gegeben, die Nutzung des Dienstes mit deaktiviertem Javascript unmöglich zu machen. Der gesamte Inhalt der Website ist encoded und wird mit Javascript geschrieben.

Die IP-Adressen der Nutzer werden bei aktiviertem Javascript gleich an drei Datensammler verschickt. Neben Google Analytics erhalten auch xtendmedia.com und yieldmanager.com diese Information. Google Analytics ist bekannt, die beiden anderen Datensammler sind ebenfalls Anbieter von Werbung. Die Website enthält keinen Hinweis auf die Datenweitergabe. Zumindest im Fall von Google Analytics besteht jedoch eine Informationspflicht.

Die Ereignisse rund um den Sahra-Palin-Hack zeigen, dass auch der Dienst selbst Informationen über die Nutzer speichert. Die Kommunikationsdaten werden selbst bei kleinen Vergehen an Behörden weitergegeben. Eine seltsame Auffassung von Anonymität.

11.3.3 Free Hide IP

Free Hide IP wird von *Computerbild* als Anonymisierungsdienst angepriesen.

> *Mit Free Hide IP bleiben Sie beim Surfen im Internet anonym. So sind Sie vor Datensammlern und anderen Gefahren geschützt. Die Free-Version der Software verbindet Sie nach einem Klick auf die Schaltfläche Hide IP mit einem amerikanischen Proxy-Server und vergibt eine neue IP-Adresse für Ihren Rechner.*

Der Dienst erfüllt nicht einmal einfachste Anforderungen. Nutzer können in mehreren Varianten deanonymisiert werden - beispielsweise ganz einfach mit (verborgenen) HTTPS-Links.

Als Tool zur Umgehung von Zensur ist der Dienst auch nicht geeignet. Die amerikanischen Proxy-Server setzen das Filtersystem *Barracuda* ein und es werden die Internetsperren des COICA-Zensurgesetzes umgesetzt.

11.3.4 ZenMate

ZenMate will ein VPN-artiger Anonymisierungsdienst sein, der eine einfach zu installierende Lösung für anonymes Surfen verspricht. Man muss auf der Webseite nur einmal kurz klicken, um einen Browser Add-on zu installieren. Es gibt eine kostenlose Version, die nur die IP-Adresse versteckt. Außerdem steht eine Premium Version zur Verfügung, die auch Tracking Elemente blockieren können soll.

Die kostenfreie Version hat Jens Kubiziel schon 2014 getestet. Das Ergebnis kann man einfach zusammenfassen: es funktioniert nicht zuverlässig.Insbesondere wenn man ZenMate zur Umgehung regionaler IP-Sperren

verwenden möchte, um Videos zu schauen, die im eigenen Land nicht verfügbar sind, funktioniert die IP-Anonymisierung NICHT.[54]

Your IP	103.10.197.58 88.130.140.38 [Flash]
Your location	Germany undefined
Your net provider	Versatel Deutschland
Reverse DNS	i58828C26.versanet.de

Abbildung 11.22: ZenMate IP-Leak via Flash

Ich habe mir die Premium Version angeschaut:

- Die Registrierung und später der Login in den Premium Dienst erfordern die Angabe einer E-Mail Adresse, was eindeutig ein identifizierendes Merkmal ist. Das gesamte anonymisierte Surfverhalten von Premium Kunden könnte ZenMate eindeutig dem Inhaber einer E-Mail Adresse zugeordnen. Vielleicht protokolliert ZenMate wirklich nichts, technisch wäre es aber einfach möglich.
- Die nächste Überraschung war die Verschmutzung der E-Mails zur Zahlungsbestätigung mit Tracking Wanzen. Wenn man die E-Mails von ZenMate genauer untersucht, findet man ein kleines, nicht sichtbares Bildchen, welches mit einer individuellen URL von einem ZenMate Tracking Server geladen wird.

  ```
  <img width="1px" height="1px" alt=""
   src="http=://email.zenmate.com/o/eJyzEOwjAMBdDTkIOqie....">
  ```

  ZenMate versucht also, die Empfänger der E-Mails zu verfolgen und jedes Öffnen der Mails soll registriert werden. In der Privacy Policy[55] von ZenMate wird dieses E-Mail Tracking nicht erwähnt.
- Das versprochene Blockieren von Third Party Tracking in der Premium Version funktioniert ebenfalls nicht. Cookies und moderne HTML5 Tracking Features von Drittseiten werden nicht zuverlässig blockiert, wenn man den Tracking Schutz aktiviert.

Schlussfolgerung: Das ist nur Abzocke mit zweifelhafter Werbung.

11.3.5 5socks.net

Im Forum der GPF tauchte vor einiger Zeit die Frage auf, was wir von *5socks.net* halten. 5socks.net ist ein Provider, der die Nutzungs von SOCKS-Proxies im Abbo anbietet.

Eine kurze Recherche brachte folgende Ergebnisse:

[54] https://kubieziel.de/blog/archives/1582-ZenMate-als-Anonymisierungsprogramm.html
[55] https://zenmate.com/privacy-policy/

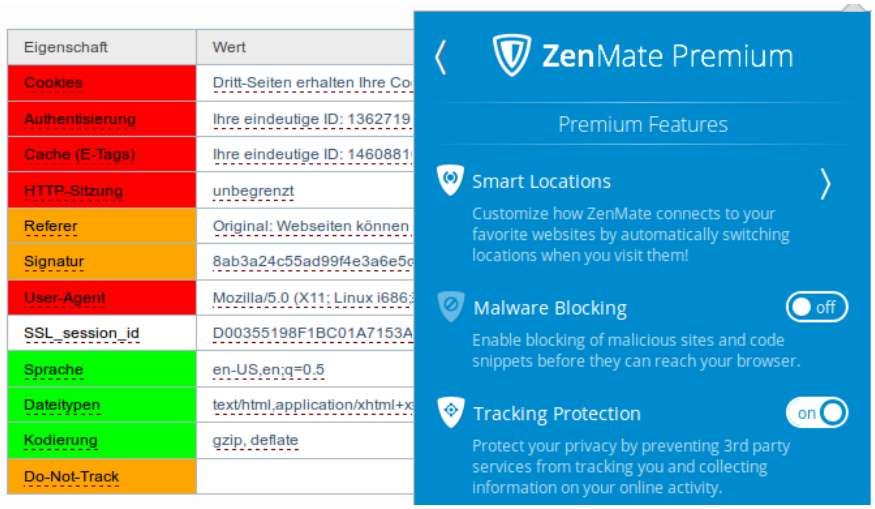


Abbildung 11.23: Tracking Protection in ZenMate funktioniert nicht

1. Fragen wir mal nach 5.socks.net:

```
domain: 5socks.net
IPv4-adress: 174.36.202.143
addr-out: s3d.reserver.ru
whois.nic.mil [0] Undefined error: 0

OrgName: SoftLayer Technologies Inc.
OrgID: SOFTL
Address: 1950 N Stemmons Freeway
City: Dallas
StateProv: TX
PostalCode: 75207
Country: US
```

2. Softlayer Technologies Inc. == Layered Technologies
   http://seo-mannsgarn.de/proxy-ip-vandalismus.htm

3. Zu dieser Firma findet man bei cryptome.info:

```
Layered Technologies Incorporated
[NSA-affiliated IP range]
Frisco TX US
72.232.0.0 - 72.233.127.255
ns2.layeredtech.com [72.232.210.195]
ns1.layeredtech.com [72.232.23.195]
```

Keiner möchte einen NSA-affiliated Anonymisierungsserver nutzen - oder?

11.3.6 BlackBelt Privacy, Cloakfish und JanusVM

Tor Onion Router ist ein populärer Anonymisierungsdienst. Der Hauptnachteil ist die geringe Geschwindigkeit. Die Entwickler von TorProject.org sind sich dieses Problems bewusst und sie arbeiten daran, die Geschwindigkeit ohne Einbußen bei der versprochenen Anonymität zu erhöhen . Daneben gibt es immer wieder ein paar Scharlatane, die mit Voodoo-Methoden eine höhere Geschwindigkeit versprechen. Ich rate davon ab, diese Projekte zu nutzen.

Tor BlackBelt Privacy verspricht durch ein bisschen Voodoo in der Konfiguration eine Erhöhung der Geschwindigkeit bei der Nutzung von Tor. Eine Analyse der Änderungen an der Konfiguration durch Tor Entwickler kommt zu dem Schluss, dass minimale Verbesserungen bei der Geschwindigkeit möglich sein könnten. Allerdings verursachen die Modifaktionen eine starke Erhöhung der Belastung des Tor Netzwerkes und sie vereinfachen Angriffe zur Reduzierung der Anonymität, wie sie auf der Defcon17 vorgestellt wurden.

Der Maintainer von BlackBelt Privacy versichert, dass die originale Software von Tor und Vidalia ohne Modifikationen am Code genutzt wird. Das kann nicht überprüft werden, da das Projekt nur Binaries für WINDOWS bereitstellt. Die Bereitstellung der *tollen torrc* würde für alle Betriebssystem ausreichen oder wäre als Ergänzung sinnvoll. Suspect.

Cloakfish ist ein Projekt, welches kommerziellen Zugriff auf das kostenfrei zugängliche Tor-Netz bieten möchte. Eine Client-Software, die als Closed-Source zum Download bereitsteht, soll vor allem SEOs ermöglichen, sich über die Tor-Exit-Nodes mit vielen verschiedenen IP-Adressen im Web zu bewegen. (laut Eigen-Werbung bis zu 15.000 verschieden Adressen pro Monat)

Durch die Verwendung von nur einem Tor-Node wird die Anonymität der Nutzer stark eingeschränkt und nicht die nächste Stufe der Anonymität erreicht, wie ein schnell aufgezogenes Werbe-Blog suggerieren möchte.

Die Tor-Entwickler missbilligen diese Nutzung des Tor-Netzwerkes, da die Load-Balancing Algorithmen von Tor durch diese Software gestört werden. Entgegen der Behauptung auf der Projekt-Webseite sind die Entwickler von Cloakfish den Tor Developern unbekannt.

Diskussionen zu Cloakfish und verunglückte Beispiele von Postings, die unter falschem Pseudonym Werbung für die Software machen wollen, findet man bei gulli, im Forum der GPF und im Forum von JonDonym. Die Software wird bei den Black SEO intensiv beworben.

JanusVM ist eine VMware Appliance für anonymes Surfen. Die Appliance soll mit openVPN, Tor, Privoxy usw. eine schlüsselfertige Lösung bieten. Roger Dingledine von TorProject.org kommentierte die JanusVM im Dezember 2011 auf der OR-Talk Liste mit folgenden Worten:

> *"Probably has been unsafe to use for years."*

11.3.7 Proxy-Listen

In der Anfangszeit des Internets nutzten Cypherpunks die Möglichkeit, ihre IP-Adresse mit mehreren Proxies zu verschleiern. Der Datenverkehr wird über ständig wechselnde Proxies geleitet, so dass der Webserver ständig eine andere IP-Adresse sieht. Es gibt Tools, die diesen Vorgang automatisieren.

Der Vorteil liegt in der im Vergleich zu Mixkaskaden und Onion-Routern höheren Geschwindigkeit. Der offensichtliche Nachteil ist, dass der Datenverkehr zwischen eigenem Rechner und den Proxies meist unverschlüsselt ist.

Inzwischen ist diese Idee häufig pervertiert worden. Im Internet kursierende Proxylisten sind alles andere als anonym. So wurde beispielsweise im Mai 2007 in der Newsgruppe *alt.privacy.anon-server* eine Liste gepostet, die mit verschiedenen DNS-Namen für Proxies gut gefüllt war. Eine Überprüfung der Liste ergab, dass hinter allen die gleiche IP-Adresse und somit derselbe Server steckt. Der Betreiber des Servers erhält eine website-übergreifende Zusammenfassung des Surfverhaltens der Nutzer!

Kapitel 12

Anonyme Peer-2-Peer Netzwerke

Anonyme Peer-2-Peer Netze nutzen die Infrastruktur des WWW, um in einer darüber liegenden komplett verschlüsselten Transportschicht ein anonymes Kommunikationsnetz zu bilden. Der Datenverkehr wird mehrfach verschlüssellt über ständig wechselnde Teilnehmer des Netzes geleitet. Der eigene Rechner ist auch ständig an der Weiterleitung von Daten für andere Teilnehmer beteiligt. Das macht die Beobachtung durch Dritte nahezu unmöglich.

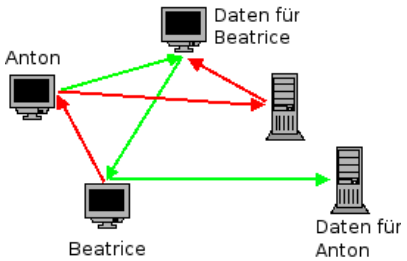


Abbildung 12.1: Prinzip von anonymen Peer-2-Peer Netzen

Hauptverwendungszweck für anonyme Peer-2-Peer Netze ist unbestritten das abmahnsichere Tauschen von Dateien. Unbeobachtete Kommunikation zwischen den Teilnehmern (E-Mail, Chatten...) ist ebenfalls möglich. Außerdem kann man zensurresistent Webseiten publizieren. Da die Nutzung der Angebote mit technischen Hürden verbunden ist, werden sie deutlich weniger besucht als klassische Webseiten.

Invisible Internet Project (I2P)

I2P hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel läßt sich nur in einem geschlossenen Netz verwirklichen. Die innerhalb des Invisible Internet bereitgestellten Ange-

bote sind nicht lokalisierbar. Wie im normalen Internet sind die meisten Angebote Server-basiert.

- Webserver stellen die sogenannten *eepsites* bereit, die Webseiten mit der Toplevel Domain *.i2p*. Es gibt Suchmaschinen für die *eepsites*. Das Äquivalent für Google ist http://eepsites.i2p.
- Als E-Mail Dienst hat sich *SusiMail* etabliert, ein zentraler Mailserver für I2P mit Gateway ins normale Internet. Eine neue Alternative ist das serverlose Projekt *I2P-Bote*.
- Das Äquivalent zum Usenet ist *Syndie*. Es gibt öffentliche und private Diskussionsforen, die auf Syndicationservern gehostet werden.
- Es gibt zwei redundante Server für IRC.
- Für das Filesharing ist mit *I2Psnark* eine Adaption von BitTorrent vorhanden. Der Tracker von *Postman* ist das Äquivalent zur PirateBay im normalen Netz.

Freenet

Freenet bietet Schutz gegen das umfangreichste Angriffsmodell. Freie Kommunikation unter den Bedingungen globaler Überwachung ist das Ziel des Projektes. Es stellt die höchsten Anforderungen an die Nutzer und erzielt die langsamsten Downloadraten.

Im Unterschied zu I2P werden die Inhalte im Freenet redundant über alle Peers verteilt und verschlüsselt abgelegt. Es gibt keine Server für Webdienste, E-Mail usw. Der Zugriff auf die Inhalte erfolgt nicht über einfache URLs, sondern über komplexe Schlüssel, welche die Adressen der TOR Hidden Services als absolut harmlos erscheinen lassen. Einmal veröffentlichte Inhalte können im Freenet nicht mehr modifiziert werden, auch nicht vom Autor. Es ist jedoch möglich, aktualisierte Versionen zu veröffentlichen. Die Freenet Software stellt sicher, dass immer die aktuellste Version angezeigt wird.

Neben Webseiten gibt es *F-Mail* und mit *Frost* ein Äquivalent zum Usenet. Das Tauschen von Dateien erfolgt direkt im Browser mit einer Oberfläche, die der Freenet-Knoten bereitstellt.

Unabhängig vom *Open Freenet* kann man mit vertrauenswürdigen Freunden ein eigenes Netz konfigurieren, welches sich vollständig der Beobachtung durch Dritte entzieht.

12.1 Invisible Internet Project (I2P)

Das Invisible Internet Project (I2P) hat das Ziel, Anonymität sowohl für Konsumenten als auch für Anbieter von Angeboten zu bieten. Dieses Ziel lässt sich nur in einem geschlossenen Netz verwirklichen.

Das Projekt bietet einen Java-basierten Client. Dieser Client verschlüsselt den Datenverkehr für alle Internet-Anwendungen, die I2P nutzen. Außerdem stellt er sicher, dass ständig neue Verbindungen zu anderen Rechnern des Netzwerkes aufgebaut werden.

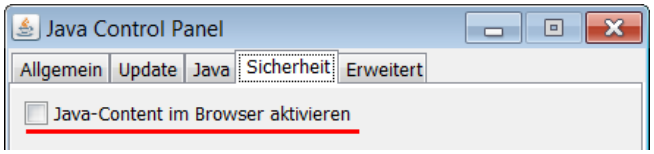
Neben der Möglichkeit, anonym zu surfen und Websites (sogenannte *eep-sites*) anzubieten, sind weitere Anwendungen bereits fester Bestandteil von I2P. Es bietet anonyme E-Mail (Susimail, I2P-Bote), BitTorrent Downloads (I2Psnark), ein anonymes Usenet (Syndie) u.a.m.

12.1.1 Installation des I2P-Routers

Für die Nutzung des Invisible Internet Projects benötigt man den I2P-Router, der als Proxy für verschiedene Anwendungen (Webbrowser, E-Mail Client...) dient und die Weiterleitung der Daten vom und zum I2P-Netz übernimmt. Der I2P-Router ist eine Java-Applikation und steht unter https://geti2p.net/de zum Download bereit.

Windows: Als erstes ist ein Java-Runtime-Environment (JRE) zu installieren. Das Installationsprogramm für Java gibt auf der Webseite www.java.com[1]. Der Installer möchte unbedingt die *Ask-Toolbar* für alle Browser installieren. Das sollte man deaktivieren, braucht man nicht.

WICHTIG: Der Installer aktiviert auch ein Java-Plugin für alle Browser. Dieses Plug-in ist ein Sicherheitsrisiko und muss im Java Control Panel unter *Systemsteuerung - Programme - Java* deaktiviert werden!



Anschließend kann der I2P-Router installiert werden. Die Datei *i2pinstall-0.x.y.exe* von der I2P Downloadseite enthält einen kompletten Installer, der nach dem Start alles Nötige einrichtet. Einfach starten und dem Assistenten folgen. Nach der Installation findet man im Startmenü die neue Gruppe *I2P* (Bild 12.2).

[1] http://www.java.com/de/

Abbildung 12.2: I2P im Startmenü von Windows

Die beiden Punkte zum Starten von I2P unterscheiden sich nur gering. Im ersten Fall hat man keine störende Konsole auf dem Desktop. *I2P router console* öffnet den Webbrowser, um den Router zu konfigurieren oder abzuschalten mit der Adresse http://localhost:7657.

Ubuntu: Für Ubuntu kann man das offizielle PPA Repository der I2P Maintainer nutzen. Dieses Repository enthält nur den I2P-Router. Es wird mit folgenden Kommandos aktiviert und danach der I2P-Router installiert:

```
> sudo apt-add-repository ppa:i2p-maintainers/i2p
> sudo apt update
> sudo apt install i2p
```

Debian: Auch für Debian gibt es ein Repository, das man mit folgenden Zeilen in der Datei */etc/apt/sources.lst* einbindet:

```
deb http://deb.i2p2.no/ stable main
deb-src http://deb.i2p2.no/ stable main
```

Außerdem ist der Signaturschlüssel des Repository *i2p-debian-repo.key.asc* herunterzuladen und in den Apt-Keyring einzufügen mit:

```
> wget https://geti2p.net/_static/i2p-debian-repo.key.asc
> sudo apt-key add i2p-debian-repo.key.asc
```

Danach kann man I2P und auch das Paket *i2p-keyring* für spätere Updates des Signaturschlüssels installieren:

```
> sudo apt install i2p i2p-keyring
```

Linux: Als erstes ist Java (Paket: *default-jre*) mit der Paketverwaltung der Distribution zu installieren. Danach kann der I2P-Router installiert werden. Den Installer *i2pinstall-0.x.y.jar* findet man auf der Downloadseite des Projektes. Nach dem Downlad startet man den Installer und wählt die Sprache sowie das Verzeichnis für die Installation:

```
> java -jar i2pinstall-*.jar
```

In dem neu angelegten Installationsverzeichnis findet man das Script zum Starten/Stoppen des I2P-Routers:

```
> ~/i2p/i2prouter start
```

Stoppen lässt sich der Router in der Router-Konsole im Webbrowser unter http://localhost:7657 mit Klick auf den Link *shutdown* oder obiges Kommando mit der Option *stop*.

Linux (advanced): K. Raven hat eine umfassende Anleitung geschrieben, wie man den I2P-Router in einer chroot-Umgebung installiert und mit AppArmor zusätzlich absichert. Lesenswert für alle, die es richtig gut machen wollen. Link: http://wiki.kairaven.de/open/anon/chrooti2p

Nach dem ersten Start braucht der I2P-Router einige Zeit, um sich im Invisible Internet zu orientieren. Zum Warmlaufen sollte man ihm 30 min Zeit lassen. Wenn es danach noch immer nicht so richtig funktioniert, sind die Netzwerkeinstellungen zu prüfen. Die Startseite der Router-Console gibt einige Hinweise.

Den I2P-Router kann man nicht kurz einmal starten, wenn man ihn nutzen möchte. Er sollte möglichst immer laufen, wenn der Rechner online ist. Damit lernt er die verfügbaren Peers und eepsites besser kennen und ist besser in das Netz eingebunden.

12.1.2 Konfiguration des I2P-Router

Standardmäßig ist der I2P-Router funktionsfähig vorkonfiguriert. Ein paar kleine Anpassungen können die Arbeit etwas verbessern.

Bandbreite anpassen

Der I2P-Router arbeitet am besten, wenn man die Bandbreite an den eigenen Internetanschluss anpasst. Nach dem Start kann man auf der Seite http://localhost:7657/config der Router Konsole die Werte anpassen.

Netzwerkkonfiguration

Auf der Seite http://localhost:7657/confignet der Router Konsole sind die Einstellungen für die Einbindung in das I2P-Netz zu konfigurieren. Dabei gibt es zwei Möglichkeiten:

1. Wenn der eigene Rechner nicht vom Internet erreichbar ist, dann sind folgende Optionen zu aktivieren, damit der I2P-Router korrekt arbeitet:
   - *Versteckter Modus* ist zu aktivieren.
   - Optional kann der *Laptop Modus* aktiviert werden. Dann ändert sich Router-Identifikation bei Änderung der IP-Adresse.
2. Wenn der eigene I2P-Router vom Internet für andere Teilnehmer erreichbar ist, verbessert sich die Performance und Anonymität. In der Netzwerk Konfiguration des I2P-Routers sind dann folgende Optionen zu konfigurieren:
   - UPnP ist aus Sicherheitsgründen auf dem DSL-Router zu deaktivieren. Damit ist klar, dass in der Netzwerkkonfiguration des I2P-Routers das *UPnP Portforwarding* und die *UPnP IP-Adresserkennung* auch zu deaktivieren sind.

- In den UDP-Einstellungen ist der Port anzugeben, für den die Weiterleitung auf dem DSL-Router konfiguriert wurde.
- In den TCP-Einstellungen ist ebenfalls der Port zu konfigurieren und die Option *automatisch erkannte IP-Adresse benutzen* zu aktivieren.

Die Hinweise im Kapitel *Konfiguration des DSL-Routers* erläutern die notwendigen Einstellungen, damit Ihr Rechner vom Internet erreichbar ist. Auf dem DSL-Router ist ein Portforwarding zu Ihrem Rechner zu konfigurieren und die Firewall des Rechners ist anzupassen.

SusiDNS anpassen

Für die Zuordnung von Domainnamen mit der Toplevel Domain .i2p zu einem Service wird SusiDNS verwendet, ein dem DNS im Internet vergleichbares System. Wie in den Anfangszeiten des WWW erhält jeder I2P Router eine komplette Liste der bekannten eepsites: das *addressbook*.

Um neue eepsites oder Services in das addressbook einzufügen, verwendet I2P sogenannte *subscriptions*. Die eine standardmäßig vorhandene subscription wird relativ selten aktualisiert.

Um auf dem Laufenden zu bleiben, kann man weitere subscriptions zu abonnieren. Die Einstellungen für SusiDNS findet man in der Routerkonsole. Subscriptions kann man unter folgender Adresse einfügen: http://localhost:7657/susidns/subscriptions.jsp (Bild 12.3)

Abbildung 12.3: subscriptions für SusiDNS

Folgende subscriptions bieten aktuelle Neuerscheinungen von eepsites:

```
http://stats.i2p/cgi-bin/newhosts.txt
http://i2host.i2p/cgi-bin/i2hostetag
```

```
http://tino.i2p/hosts.txt
```

12.1.3 Anonym Surfen mit I2P

Der I2P-Router stellt einen HTTP- und HTTPS-Proxy für den Webbrowser bereit. Die Default-Adressen dieser Proxys sind:

```
          Rechner:  localhost
    HTTP-Proxy Port:  4444
     SSL-Proxy Port:  4445
     FTP-Proxy Port:  4444
  Gopher-Proxy Port:  4444
```

Der Proxy kann genutzt werden, um Webseiten im Invisible Internet aufzurufen (sogenannte *eepsites*, erkennbar an der Toplevel Domain **.i2p**).

JonDoFox nutzen

Das Firefox Profil *JonDoFox* ist für spurenarmes und sicheres Surfen optimiert. Es bietet neben *JonDo* und *Tor* eine *Benutzerdefinierte Proxy Konfiguration*, die man für I2P nutzen kann. Die Einstellungen zeigt Bild 12.4. Der JonDoFox verhindert zuverlässig eine Kompromittierung der Anonymität.

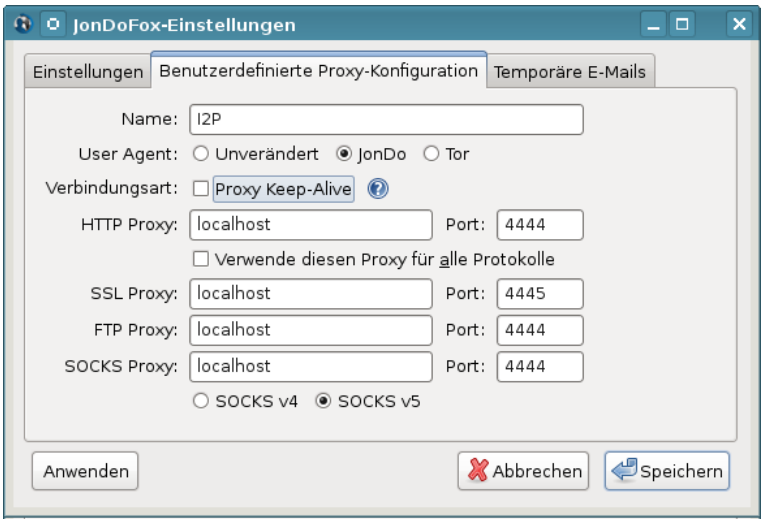


Abbildung 12.4: Benutzerdefinierte Proxy Konfiguration im JonDoFox

Firefox selbst konfigurieren

Ich würde empfehlen, für das Surfen im Invisible Internet ein separates Firefox-Profil zu erstellen. Dann ist es für spionierende Websites gänzlich unmöglich, im Cache oder in der Historie abgelegte Daten über das anonyme Surfen auszulesen. Den Profil-Manager von Firefox startet man mit folgendem Kommando:

```
> firefox -P
```

In dem sich öffnenden Dialog (Bild 12.5) kann man ein neues Profil anlegen und anschließend die Proxy-Einstellungen konfigurieren. In Zukunft wird Firefox bei jedem Start fragen, welches Profil genutzt werden soll.

Abbildung 12.5: Firefox Profil-Manager

Anschließend kann das Profil *I2P-Fox* gestartet werden und die Proxy-Einstellungen sind wie im Bild 12.6 gezeigt zu konfigurieren. Die allgemeinen Hinweise zu Cookies, Javascript, Plug-ins, HTTPS-Security usw. im Abschnitt *Spurenarm Surfen* gelten auch für I2P. Das Profil *I2P-Fox* ist entsprechend zu konfigurieren.

Wichtige Sicherheitseinstellungen für Firefox

Flash und Java Plug-ins sind unbedingt zu deaktivieren, da diese Plug-ins die Proxy Einstellungen umgehen könnten. Um eine Deanonymisierung zu vermeiden, sind für einen aktuellen Firefox außerdem folgende Features unter der Adresse *about:config* zu deativieren:

- WebRTC kann durch UDP-Tunnel die reale IP-Adresse aufdecken (nur Firefox 18 und neuer):

  ```
  media.peerconnection.enabled = false
  ```

- Geolocation-API kann den realen Standort ermitteln:

  ```
  geo.enabled = false
  ```

- Phishing- und Malware Protection funktioniert für eepsites nicht, da die Webseiten des Darknet nicht in der Google Datenbank enthalten sind:

  ```
  browser.safebrowsing.enabled = false
  ```

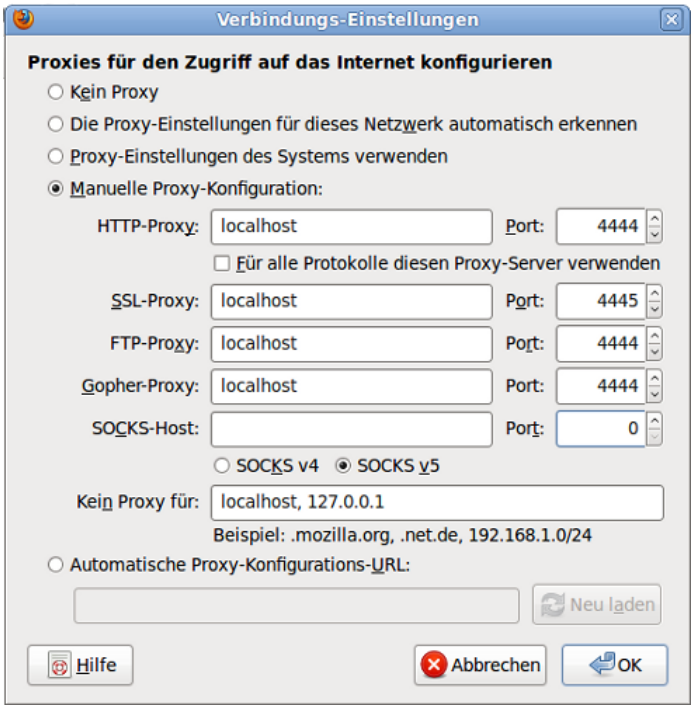


Abbildung 12.6: Firefox Proxy-Einstellungen für I2P

Suchmaschinen für I2P

Um sich in einem Netzwerk zu orientieren, braucht man eine Suchmaschine. Die Webseite plugins.i2p bietet viele *Firefox Search Plugins für I2P*. Wenn man die Webseite http://plugins.i2p/firefox aufgerufen hat, kann man die Suchmaschinen einfach durch Aufklappen der Liste der Suchmaschinen oben rechts im Firefox hinzufügen. Unter dem Trennstrich findet man die neuen Suchmaschinen, die diese Webseite zur Installation anbietet.

Das Äquivalent zu Google im normalen Internet ist im I2P-Netz die Suchmaschine http://eepsites.i2p. Die anderen Dienste in der Liste durchsuchen einzelne eepsites.

12.1.4 I2P Mail 1 (Susimail)

Die Anwendung Susimail ist integraler Bestandteil von I2P und ermöglicht den unbeobachteten Austausch von E-Mails. Das Anlegen und Verwalten eines Susimail-Accounts erfolgt auf der eepsite http://hq.postman.i2p.

Es ist möglich, E-Mails in das normale Web zu versenden und auch von dort unter der Adresse *<username>@i2pmail.org* zu empfangen. die Weiterleitung ins normale Internet kann bis zu 24h dauern und ist von den gewählten Einstellungen auf HQ Postmaster abhängig. Um für Spammer unattraktiv zu

sein, haben die Entwickler von I2P die Anzahl der ins normale Web versendbaren Mails begrenzt. Es ist möglich, innerhalb von 24h bis zu 20 Emfängern beliebig viele E-Mail zu senden. Wer unbedingt mehr Leute per E-Mail kontaktieren will, kann mit einem Hashcash ein Kontingent von weiteren 20, 40 oder 80 Empfängern freischalten.

Routerkonsole nutzen

Ein einfaches Webinterface für Susimail ist in der I2P Routerkonsole erreichbar unter der Adresse http://localhost:7657/susimail/susimail.

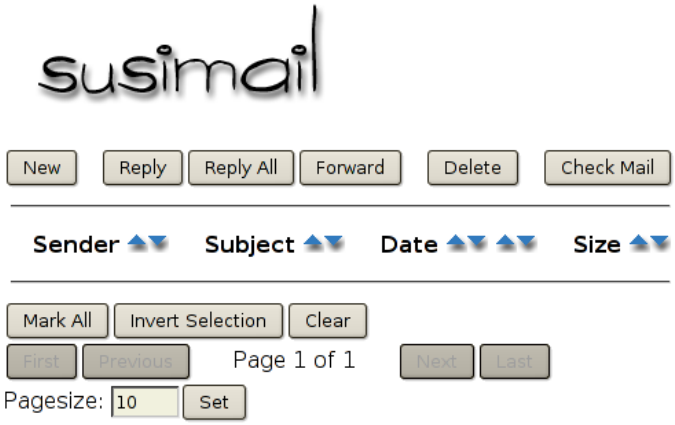


Abbildung 12.7: Webinterface von Susimail

Es bietet eine simple Möglichkeit, Mails abzurufen und zu versenden. Komfortabler ist die Nutzung des bevorzugten E-Mail Clients, vor allem wenn man die Möglichkeiten zur Verschlüsselung der Nachrichten nutzen möchte.

Thunderbird konfigurieren

Der Susimail-Account kann mit jedem E-Mail Client genutzt werden.

```
SMTP-Server: localhost    Port: 7659
POP3-Server: localhost    Port: 7660
Login-Name:  <username>
```

In Thunderbird ist als erstes ein neuer SMTP-Server anzulegen (Konten -> Postausgangs-Server (SMTP) -> Hinzufügen). Der Server erfordert eine Authentifizierung mit den Daten des Susimail Accounts.

Danach kann ein neues POP3-Konto angelegt werden, welches diesen SMTP-Server für die Versendung nutzt. SSL- und TLS-Verschlüsselung sind zu deaktivieren. Der I2P-Router übernimmt die abhörsichere Übertragung.

In den Server-Einstellungen des Kontos sollte die Option *"Alle x Minuten auf neue Nachrichten prüfen"* deaktiviert werden! Die Admins von Susimail bitten darum, den Service nicht unnötig zu belasten.

Susimail mit Tor nutzen

An Stelle des I2P-Routers kann auch Tor für den Abruf und das Versenden von Nachrichten via I2P Mail genutzt werden. Folgende Hidden Services bieten ein SMTP-Gateway (Port: 7659) und POP3-Gateway (Port: 7660):

```
v6ni63jd2tt2keb5.onion
5rw56roal3f2riwj.onion
```

Die Hidden Service Adresse ist als SMTP- und POP3-Server im E-Mail Client für das I2P-Mail-Konto an Stelle von *localhost* einzutragen. Außerdem ist der E-Mail Client so zu konfigurieren, dass er Tor als Proxy nutzt. Sollte der E-Mail Client ständig den Fehler TIMEOUT liefern, hilft es, den Hidden Service erst einmal im Webbrowser aufzurufen.

Hinweise zur Nutzung von Susimail

Der Service wird von *postman* und *mastijaner* in der Freizeit aufgebaut und gepflegt. Sie bitten darum, folgene Hinweise zu beachten:

1. Bitte nicht den POP3-Service in kurzen Intervallen automatisiert abfragen. Einige Nutzer fragen den POP3-Dienst immer wieder innerhalb weniger Minuten ab und belasten den Service stark. Zweimal pro Tag sollte reichen.

2. Um anonym zu bleiben, sollte man keine Mails an die eigene Mail Adresse im Web schreiben oder an Bekannte, mit denen man via E-Mail im normalen Web Kontakt hält.

3. Bitte Susimail nicht für Mailinglisten nutzen, die man nicht mitliest. Das Abmelden auf Mailinglisten bei Desinteresse nicht vergessen.

4. Wer nicht mehr im Invisible Internet aktiv ist, sollte auch an das Löschen des Susimail Account denken. Scheinbar gibt es auf dem Server viele tote Mail-Accounts, wo noch immer Mails eingehen (Spam und Mailinglisten) und viel Speicherplatz verbrauchen.

5. Bitte verwendet den Dienst nicht, um anonyme Beleidigungen oder Drohungen zu schreiben. Das bringt den Betreibern Ärger und gefährdet den reibungslosen Betrieb.

Englischer Orginaltext bei HQ Postman: http://hq.postman.i2p/?p=63

12.1.5 I2P Mail 2 (Bote)

I2P Bote bietet serverlose und verschlüsselte E-Mail Kommunikation. Die Daten werden redundant und verschlüsselt in einer DHT gespeichert, über alle Teilnehmer verteilt. Es gibt keinen zentralen Server, der Kommunikationsprofile erstellen oder eine Vorratsdatenspeicherung umsetzen könnte. Starke

Kryptografie stellt sicher, dass nur der Empfänger die Nachricht lesen kann.

I2P Bote ist keine Weiterentwicklung von Susimail und es soll es auch nicht ersetzen. Langfristig werden beide Projekte parallel existieren und kooperieren. Das Projekt bietet folgende Features:

- Bedienung im Webinterface der I2P-Routerkonsole.
- Erzeugen von Identitäten, Senden/Empfangen von E-Mails.
- SMTP- und IMAP-Gateway für die Integration in Thunderbird u.a.
- Anonyme Absender und Versenden über Zwischenstationen mit zeitlicher Verzögerung (Remailer-Konzept).
- Dateianhänge bis 500 kB werden unterstützt. Die Begrenzung der Größe der Dateianhänge ist aufgrund der redundanten Speicherung nötig. Die Nachrichten werden mit 20x Redundanz gespeichert und eine 1 MB große Mail würde 20 MB Speicherplatz in der DHT belegen.

Installation von I2P Bote

Um I2P Bote zu nutzen, ist die Installation von 3 Plug-ins für den I2P Router nötig. Auf der Seite I2P Dienste der Routerkonsole (unter http://localhost:7657/configclients.jsp) findet man ganz unten den Abschnitt für die Installation zusätzlicher Plug-Ins (Bild 12.8).

Abbildung 12.8: Installation des Plug-in I2P Bote

Folgende Plug-Ins sind in dieser Reihenfolge zu installieren:

1. http://sponge.i2p/files/seedless/01_neodatis.xpi2p

2. http://sponge.i2p/files/seedless/02_seedless.xpi2p
3. http://i2pbote.i2p/i2pbote.xpi2p

Nach erfolgreicher Installation findet man auf der Startseite in der Liste der *Lokalen Dienste* oder rechts im Menü der Routerkonsole einen neuen I2P Dienst *SecureMail*. Ein Klick öffnet die Web-Oberfläche in einem neuen Browser-Tab.

Eigene Identität erzeugen

Der erste Schritt nach der Installation ist in der Regel die Erstellung einer eigenen Adresse. In der Navigationsleiste rechts wählt man *"Identitäten"* und den Button *"Neue Identität"*.

Als Pflichtfeld ist nur ein Name anzugeben. Die Verschlüsselung belässt man am besten bei 256Bit-ECC. Diese Verschlüsselung liefert relativ kurze und starke Schlüssel. Die Mailadresse wird zur Zeit noch nicht genutzt.

Die kryptische Bote-Adresse ist an alle Partner zu verteilen oder zu veröffentlichen. In der Übersicht ist die Adresse nicht voll sichtbar. Wenn man auf die Identität klickt, erhält man eine vollständige Ansicht. Die gesammelten Adressen der Partner können in einem rudimentären Adressbuch verwaltet werden.

Abbildung 12.9: Neue Identät für I2P-Bote anlegen

Konfiguration

Bevor man loslegt, sollte man einen Blick in die Konfiguration werfen und diese anpassen.

- Abrufen der Nachrichten: Es ist konfigurierbar, ob und in welchem Intervall neue Nachrichten aus der DHT automatisch abgerufen werden sollen. Um die Belastung des Bote-Netzes gering zu halten sollte man Intervalle von 2-3h nutzen. Bei Bedarf kann man das Abrufen neuer Nachrichten auch selbst anstoßen.
- Über Zwischenstationen senden: Wird diese Option deaktiviert ("AUS"), gehen versendete Nachrichten direkt in die DHT. Die Anonymität

entspricht der normalen Anonymität bei der Nutzung von I2P.

Eine höhere Anonymität erreicht man, wenn die Nachricht vor dem Speichern in der DHT über 1...n Teilnehmer des I2P-Bote Netzes geleitet und dort jeweils um eine zufällige Zeitspanne verzögert wird. Die min. und max. Werte für die Verzögerung können konfiguriert werden. Ähnlich wie bei Remailern sinkt damit natürlich die Performance der Kommunikation.

- Durchleitung an Nicht-I2P-Adressen: Es ist möglich, Mails an Nicht-I2P-Bote Teilnehmer zu versenden. Die Nachrichten werden an die Bote-Adresse eines Durchleitungsdienstes versendet, der sich dann um die weitere Zustellung kümmert. Derzeit arbeitet HQ Postman an der Entwicklung dieses Services, der aber noch nicht arbeitsfähig ist.
- Absendezeit: Die Absendezeit sollte man nicht mit versenden, wenn die Nachricht über Zwischenstationen gesendet wird. Anderenfalls ist es ein Feature, dass die Anonymität nur geringfügig erhöhen kann, wenn diese Option deaktiviert wird. Mir hilft es, den Überblick in der Inbox zu behalten, wenn ein Zeitstempel vorhanden ist.

Mails schreiben und empfangen

Das im Bild 12.10 gezeigte Formular für eine neue Mail öffnet sich mit Klick auf den Button *"Neu"*.

Abbildung 12.10: Neue E-Mail in I2P Bote schreiben

Als Absender kann man *Anonym* wählen, oder eine der zuvor angelegten Identitäten. Wer *Anonym* wählt, sollte sich nicht wundern, dass er vom Empfänger als anonymer Unbekannter behandelt wird. Für vertrauliche Konversation muss man seinen Gegenüber verifizieren können.

In die Felder *An*, *Kopie* oder *Blindkopie* sind die kryptischen Bote-Adressen der Empfänger einzutragen, der Rest sollte sich selbst erklären. Eingehende Mails findet man im Ordner *Posteingang*.

Adressbuch

Das Web-Interface bietet ein einfaches Adressbuch. Man kann die Bote-Adressen und Namen von Partnern sammeln und beim Schreiben einer Mail mit zwei Klicks übernehmen.

Außerdem hilft das Adressbuch bei der Verifikation der Absender empfangener Nachrichten. Ein Absender ist eindeutig nur durch seine Bote-Adresse bestimmt. Der Name kann frei gewählt werden und kann auch mehrfach genutzt werden. Es könnte also jemand den Namen HungryHobo nutzen, um sich als Hauptentwickler von I2P-Bote auszugeben.

Ein Vergleich der Bote-Adressen ist nicht intuitiv. Das Adressbuch kann diese Aufgabe übernehmen. Ist der Absender einer Nachricht im Adressbuch enthalten und stimmt die Bote-Adresse überein, dann zeigt die Liste der Inbox ein Häckchen in der Spalte **Bek**.

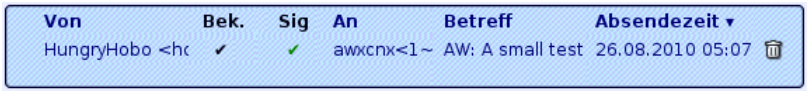


Abbildung 12.11: Inbox mit verifiziertem Absender

12.1.6 I2P IRC

IRC ist ein öffentlicher Chat Service. Auf den IRC-Servern gibt es verschiedene Chat-Räume, sogenannte Channels, in denen man sich zu einem bestimmten Thema austauschen kann. Die Unterhaltung ist in der Regel öffentlich, aber auch private Nachrichten können zwischen Nutzern ausgetauscht werden.

Das I2P-Netz bietet zwei anonyme Chat-Server, die direkt über den I2P-Router erreichbar sind. Die Konfiguration der verschiedenen Clients wie XChat (Linux/UNIX), Kopete (KDE), Colloquy (MacOS) oder Mirc (Windows) ist einfach. Man nutzt als Chat-Server folgende Adresse und ist anonym:

```
Host: localhost
Port: 6668
```

Die wichtigsten Chat-Kommandos

Der Chat wird in der Regeln komplett durch Kommandos gesteuert. Alle Kommandos beginnen mit einem Slash. Eine kurze Liste der wichtigsten Kommandos:

/list Listet alle Diskussions-Channels auf, die auf dem Server verfügbar sind.

/join #channel Den Raum #channel betreten und mitdiskutieren.

/quit Den aktiven Raum verlassen oder vom Server abmelden.

/msg nick <text> Sendet eine Nachricht an den User *nick*.

/ignore nick Einen Troll ignorieren.

/help Beantwortet alle weiteren Fragen.

Im IRC ist man mit einem Nicknamen unterwegs. Die Nicknamen werden registriert und mit einem Passwort geschützt, damit kein Dritter einen bekannten Nicknamen nutzen kann, um sich eine Identität zu erschleichen.

Die Registrierung erfolgt mit folgendem Kommando:

```
/msg nickserv register <Password> fake-email-addr
```

Um einen registrierten Nicknamen zu nutzen, muss man sich identifizieren:

```
/msg nickserv identify <Password>
```

#anonops

Die Channels von *Anonymous* stehen auch auf den I2P-IRC Servern zur Verfügung. Für die Diskussionen in diesen Channels sollten sie die Regeln von *Anonymous* beherzigen:

Basics: Tauchen Sie in der Masse unter ohne ein besonders smarter Typ sein zu wollen. Es gibt keine Helden, die alt geworden sind, es gibt nur junge Helden und "tote" Helden.

Geben Sie keine persönlichen Informationen im public IRC preis.

- keine Anhaltspunkte im Nicknamen und Realnamen veröffentlichen
- keine persönlichen Informationen im Chat diskutieren
- keine Informationen über die Herkunft diskutieren (Land, Stadt usw.)
- keine Beschreibung von Tattoos, Piercings oder anderer Merkmale
- keine Informationen über Beruf und Hobbys
- keine Sonderzeichen wie äöü verwenden, die nur in Ihrer Sprache verfügbar sind
- veröffentlichen Sie nichts im normalen Netz, während Sie in einem anonymen Chat sind - es kann einfach korreliert werden
- posten Sie keine Bilder von Facebook im Chat, diese Bilder enthalten die persönliche ID
- verbinden Sie sich nicht Tag für Tag zur gleichen Zeit mit dem Chat

12.1.7 I2P BitTorrent

Der I2P-Router bietet auch eine angepasste Implementierung des BitTorent Protokolls für anonymes Peer-2-Peer Filesharing. Im Gegensatz zur Nutzung von normalem BitTorrent über Tor ist die Implementierung des Invisble Internet Project anonym und die Nutzung ausdrücklich erwünscht. Der Dienst bietet Optimierungen mit speziellen Clients.

Die I2P-Router-Konsole bietet einen einfachen BitTorrent Client als Webinterface unter *Torrents* (http://localhost:7657/i2psnark).

Die zum Tausch bereitgestellten oder heruntergeladenen Dateien findet man im Unterverzeichnis *i2psnark* der I2P-Installation. Dieses Verzeichnis sollte Lese- und Schreibrechte für alle lokalen User haben, die I2PSnark nutzen dürfen. Torrents findet man z.B. auf den eepsites http://tracker2.postman.i2p, http://crstrack.i2p/tracker oder http://tracker.welterde.i2p. Das Webinterface bietet direkte Links zu diesen eepsites.

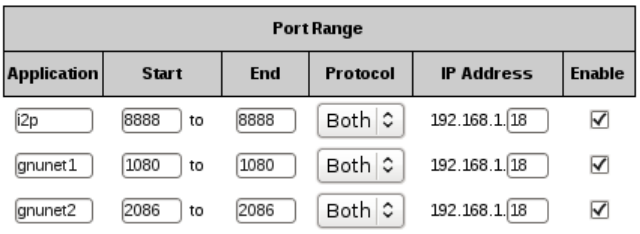
Hinweis zur Nutzung: Es gehört beim Filesharing zum guten Ton, Dateien nicht nur zu saugen. Man stellt die heruntergeladenen Dateien auch anderen Teilnehmern zur Verfügung. Bei BitTorrent im normalen Netz gilt es als freundlich, wenn man heruntergeladene Dateien mindestens für 2 Tage zum Upload anbietet oder bis die Datenmenge des Upload das 2,5fache des Downloads beträgt. Da die Geschwindigkeit im I2P-Netz wesentlich geringer ist, sollte man heruntergeladene Dateien mindestens für 1 Woche zum Upload anbieten.

12.2 DSL-Router und Computer vorbereiten

Um als vollwertiger Teilnehmer an einem anonymen Peer-2-Peer Netz teilzunehmen, muss der eigene Rechner vom Internet aus erreichbar sein. Nur dann können andere Teilnehmer des Netzes den eigenen Knoten kontaktieren. Als typischer Heimnutzer mit DSL-Anschluss sind einige Anpassungen nötig, damit der eigene Rechner aus dem Internet erreichbar ist.

1. Der DSL-Router muss den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer an den eigenen Rechner weiterleiten. Einige Programme können den Router mit UPnP konfigurieren. Aufgrund der Sicherheitsprobleme bei UPnP [2] sollte man dieses Feature auf dem Router deaktivieren und die Weiterleitung per Hand konfigurieren.

   Der Screenshot 12.12 zeigt die Konfiguration für einen Linksys Router. Für I2P wurde im Beispiel der Port 8888 gewählt, für GnuNet muss man die Ports 1080 und 2086 weiterleiten.



Port Range					
Application	Start	End	Protocol	IP Address	Enable
i2p	8888 to	8888	Both	192.168.1.18	☑
gnunet1	1080 to	1080	Both	192.168.1.18	☑
gnunet2	2086 to	2086	Both	192.168.1.18	☑

Abbildung 12.12: Portforwarding auf dem Router

2. Die Konfiguration der Weiterleitung auf dem DSL-Router ist einfacher, wenn der eigene Rechner innerhalb des privaten lokalen Netzwerkes eine feste IP-Adresse hat. Dafür ändert man die Konfiguration der Netzwerkschnittstelle von *DHCP* auf *feste IP-Adresse*.

3. Außerdem muss die Firewall auf dem lokalen Rechner den ankommenden Datenverkehr der anderen Peer-2-Peer Teilnehmer auf den Ports durchlasssen, für die eine Weiterleitung im Router konfiguriert wurde.

[2] http://heise.de/-1793625

Kapitel 13

Daten verschlüsseln

Dass die Verschlüsselung von Daten der Erhaltung der Privatsphäre dient, bemerkt man spätestens, wenn ein USB-Stick verloren geht. Wird ein Laptop gestohlen, möchte man die Fotosammlung sicher nicht im Internet sehen.

Investigative Journalisten, Rechtsanwälte und auch Priester haben das Recht und die Pflicht, ihre Informanten bzw. Klienten zu schützen. Sie sollten sich frühzeitig Gedanken über ein Konzept zur Verschlüsselung machen. Es ist wirklich ärgerlich, wenn die Rote Hilfe einen unverschlüsselten Datenträger mit Mitgliederdaten verliert. Das kann ernste Konsequenzen haben.

Als Whistleblower sind besondere Anforderungen an die Datensicherheit zu stellen. Neben der sicheren Aufbewahrung kommt es auch darauf an, keine Spuren auf den Rechnern zu hinterlassen. Im Fall Bradley Mannings konnten Forensiker viele Daten wiederherstellen.

Die kurzen Beispiele zeigen, dass unterschiedliche Anforderungen an eine Verschlüsselung bestehen können. Bevor man wild anfängt, alles irgendwie zu verschlüsseln, sollte man sich Gedanken über die Bedrohung machen, gegen die man sich schützen will:

1. **Schutz sensibler Daten** wie z.B. Passwortlisten, Revocation Certificates o.ä. erfordert die Speicherung in einem Container oder verschlüsselten Archiv, welches auch im normalen Betrieb geschlossen ist.

2. **Schutz aller persönlichen Daten** bei Verlust oder Diebstahl von Laptop oder USB-Stick erfordert eine Software, die transparent arbeitet ohne den Nutzer zu behindern und bei korrekter Anmeldung möglichst automatisch den Daten-Container öffnet (beispielsweise Veracrypt für Windows/linux oder dm-crypt für Linux).

3. **Backups auf externen Medien** enthalten in der Regel die wichtigen privaten Daten und sollten ebenfalls verschlüsselt sein. Dabei sollte die Wiederherstellung auch bei totalem Datenverlust möglich sein. Es ist nicht sinnvoll, die Daten mit einem PGP-Schlüssel zu chiffrieren, der nach einem Crash nicht mehr verfügbar ist.

4. **Daten in der Cloud** sollten ebenfalls transparent verschlüsselt werden. Außerdem sollte die Verschlüsselung die Synchronisation geänderter Dateien im Hintergrund nicht behindern. Container-basierte Lösungen wie dm-crypt oder Veracrypt sind weniger geeignet, da man bei einer kleinen Änderung nicht den gesamten Container hochladen möchte. Besser geeignet sind Verzeichnis-basierte Ansätze wie *Boxcryptor* oder *Cryptomator* (beide für Windows, MacOS, Linux und Smartphones verfügbar).

5. Wer eine **Manipulation der Systemdaten** befürchtet, kann seinen Rechner komplett verschlüsseln (z.B. mit dm-crypt für Linux).

6. **SDSRDDs** kann man nutzen, wenn Sicherheit absolute Priorität hat, Geld keine Rolle spielt und man sich nicht auf eine Softwarelösung verlassen möchte. SDSRDDs sind SSD Festplatten mit integrierter Verschlüsselung, Token-Authentifizierung (also nicht mit Keyloggern angreifbar) und eingebautem Mechanismus zur Selbstzertörung, der remote via SMS oder bei unerlaubten Zugriff ausgelöst werden kann.

13.1 Konzepte der vorgestellten Tools

Um die vorgestellten Tools sinnvoll einzusetzen, ist es nötig, die unterschiedlichen Konzepte zu verstehen.

GnuPG arbeitet Datei-orientiert. Einzenle Dateien können verschlüsselt werden. Die unverschlüsselten Orgnaldateien sind sicher(!) zu löschen, damit keine Spuren auf der Festplatte bleiben.

Cryptomator, Boxcryptor arbeiten Verzeichnis-basiert. Es werden zwei Verzeichnisse definiert:

1. Das Verzeichnis A mit den verschlüsselten Daten wird auf den Datenträger geschrieben bzw. in die Cloud synchronisiert.
2. Ein zweites Verzeichnis B oder ein virtuelles Laufwerk bietet den transparenten Zugriff auf die entschlüsselten Daten.

Veracrypt, dm-crypt arbeiten Container-basiert. Es ist zuerst ein verschlüsselter Container fester Größe zu erstellen, der dann wie ein Datenträger in das Dateisystem eingebunden werden kann. Als Container können komplette USB-Sticks, ganze Partitionen der Festplatte oder (große) Dateien genutzt werden.

Ein Container nimmt immer die gleiche Menge an Platz ein, egal ob leer oder voll. Ist der Container verschlossen, kommt niemand an die dort lagernden Daten heran. Mit einem Schlüssel kann der Container geöffnet werden (gemounted: in das Dateisystem eingefügt) und jeder, der an einem offenen Container vorbeikommt, hat Zugriff auf die dort lagernden Daten. Als Schlüssel dient eine Passphrase und/oder Schlüsseldatei(en).

Der Zugriff auf Dateien innerhalb des geöffneten Containers erfolgt mit den Standardfunktionen für das Öffnen, Schließen und Löschen von Dateien. Auch Verzeichnisse können angelegt bzw. gelöscht werden. Die Verschlüsselung erfolgt transparent ohne weiteres Zutun des Nutzers.

Veracrypt - mit doppeltem Boden

Veracrypt[1] ist ein Nachfolger des legendären Truecrypt. Es beseitigt einige Schwäche, die bei einem Audit von Truecrypt[2] aufgedeckt wurden und wird nach Open Source Prinzipien weiterentwickelt. Mit Veracrypt neu erstellte Container sind nicht kompatibel mit dem alten Truecrypt Format und können nicht mit tcplay (für Linux) geöffnet werden. Alte Truecrypt Container können aber mit Veracrypt geöffnet und weiter verwendet werden. Aus Sicherheitsgründen sollte man alle Daten in die neuen Veracrypt Container kopieren.

Ein Feature von Veracrypt und tcplay ist das Konzept des *versteckten Volumes*, eine Art doppelter Boden für den verschlüsselten Container. Der Zugriff auf diesen Bereich ist mit einem zweiten Schlüssel geschützt, einer weiteren Passphrase und/oder Schlüsseldatei(en). Öffnet man den Container mit dem ersten Schlüssel, erhält man Zugriff auf den äußeren Bereich. Verwendet man den zweiten Schlüssel zum Öffnen des Containers, erhält man Zugriff auf den versteckten Inhalt im doppelten Boden.

Während ein einfacher Container leicht als verschlüsselter Bereich erkennbar ist, kann der doppelte Boden innerhalb eines Containers ohne Kenntnis des zweiten Schlüssels nicht nachgewiesen werden. Ist man zur Herausgabe der Schlüssel gezwungen, kann man versuchen, nur den Schlüssel für den äußeren Container auszuhändigen und die Existenz des doppelten Bodens zu leugnen.

Ob es plausibel ist, die Existenz des doppelten Bodens zu leugnen, hängt von vielen Faktoren ab. Zeigt z.B. die Historie der geöffneten Dokumente einer Textverarbeitung, dass vor kurzem auf einen verschlüsselten Bereich zugegriffen wurde, und man präsentiert einen äußeren Container, dessen letzte Änderung Monate zurück liegt, trifft man wahrscheinlich auf einen verärgerten Richter. Auch der Such-Index verschiedener Programme für die Indexierung der Dokumente auf dem lokalen Rechner (WINDOWS Suche, Google Desktop Search...) liefern möglicherweise Hinweise auf den versteckten Container.

13.2 Gedanken zum Passwort

An Stelle von *Passwort* sollte man vielleicht die Bezeichnung *Passphrase* bevorzugen. Sie suggeriert, dass es auch ein wenig länger sein darf und dass Leerzeichen durchaus erlaubt sind.

Eine gute Passphrase sollte leicht merkbar aber schwer zu erraten sein. Außer Buchstaben sollte sie auch Zahlen und Sonderzeichen enthalten und etwa

[1] https://veracrypt.codeplex.com
[2] https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf

20 Zeichen lang sein. So etwas schüttelt man nicht einfach aus dem Ärmel. Wie wäre es mit folgender Phrase:

```
das geht nur %mich% _AN_
```

Zusätzlich zur Passphrase können auch Keyfiles als Schlüssel genutzt werden. Damit ist es möglich, eine Zwei-Faktor-Authentifizierung aufzubauen: eine Passphrase, die man im Kopf hat, und ein Keyfile, welches man in der Hand hat. Ein Angreifer müsste beides erlangen.

Zur Herausgabe von Passwörtern im Fall einer Beschlagnahme des Rechners oder eines verschlüsselten Datenträgers gibt es immer wieder Missverständnisse. In Deutschland gelten folgende gesetzliche Reglungen:

- Richten sich die Ermittlungen gegen den Besitzer des Rechners oder Datenträgers, muss man grundsätzlich keine Passwörter herausgeben.
- Richten sich die Ermittlungen gegen Dritte, kann man die Herausgabe von Keys verweigern, wenn man sich auf das Recht zur Zeugnisverweigerung berufen oder glaubhaft(!) versichern kann, dass man sich damit selbst belasten würde. Im Zweifel sollte man einen Anwalt konsultieren.

In Großbritannien ist es bereits anders. Gemäß dem dort seit Oktober 2007 geltendem RIPA-Act können Nutzer von Verschlüsselung unter Strafandrohung zur Herausgabe der Schlüssel gezwungen werden. Es drohen bis zu 2 Jahre Gefängnis oder Geldstrafen. Dass die Anwendung des Gesetzes nicht auf die bösen Terroristen beschränkt ist, kann man bei Heise.de nachlesen. Es wurde als erstes gegen eine Gruppe von Tierschützern angewendet.[3]

Bei Einreise in die USA sind die Grenzbehörden berechtigt, elektronische Geräte (Laptops und Smartphones) zu durchsuchen. Eine Herausgabe von Passwörtern kann ohne Durchsuchungsbeschluss nicht erzwungen werden, aber die Behörden können das Gerät zur weiteren Untersuchung einziehen, wenn man das Passwort nicht herausgeben will. Die EFF.org rät, mit einer leeren, unverschlüsselten Festplatte einzureisen und ein datenloses Handy zu nutzen.[4]

Den Polizeibehörden ist bekannt, dass es starke Verschlüsselung für Festplatten gibt, die im ausgeschalteten Zustand nicht geknackt werden kann. Deshalb sind die Festnahme Spezialisten des SEK u.ä. darin geschult, bei einer Festnahme (Polizei-Sprech: *Zugriff*) die Computer im eingeschalteten Zustand zu übernehmen und ein Backup der unverschlüsselten Daten anzufertigen.

- Ross Ulbricht (der Betreiber von Silk Road 2.0) wurde festgenommen, während er seinen Tor Hidden Service administrierte. Das FBI konnte den eingeschalten Laptop übernehmen und als Beweis die aktiven Login-Sessions auf den Servern des Drogenhandelsplatzes sicherstellen. Das war sicher kein Zufall sondern beabsichtigt.

[3] http://www.heise.de/newsticker/meldung/99313
[4] https://www.eff.org/document/defending-privacy-us-border-guide-travelers-carrying-digital-devices

- Der deutsche Betreiber eines illegalen Waffenhandels im Deep Web konnte bei der Festnahme mit dem Fuß das Stromkabel aus seinem batterielosen Laptop reißen und die Verschlüsselung damit aktivieren. Das SEK hatte aber zweifellos den Auftrag, bei der Festnahme den Laptop im eingeschalteten Zustand sicherzustellen.[5]

[5] http://motherboard.vice.com/de/read/bis-das-sek-kommt

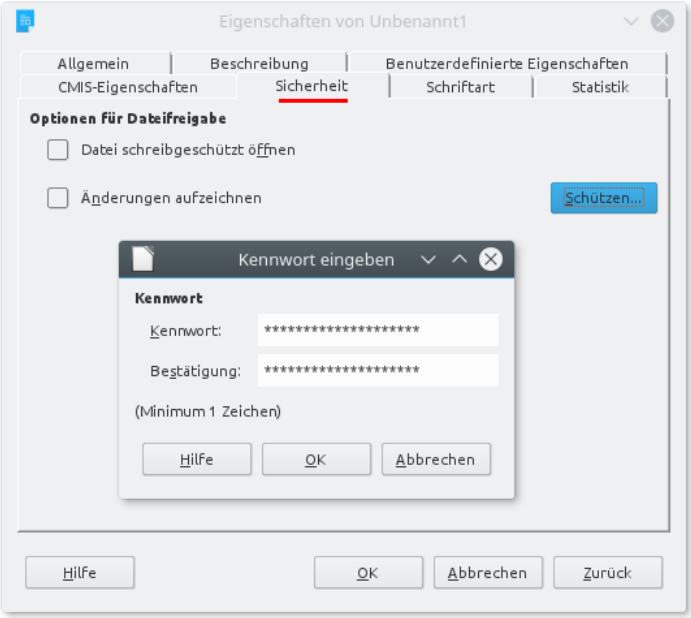


Abbildung 13.1: Verschlüsselte Speicherung in LibreOffice aktivieren

13.3 Dokumente verschlüsselt speicher

Es gibt mehrere Anwendungen, die Dokumente verschlüsselt speichern können. Das Öffnen der Dokumente ist dann nur möglich, wenn das notwendige Passwort angegeben wird. Die verschlüsselte Speicherung ist bei vertraulichen Daten sinnvoll wie z.B. Steuererklärungen, Mitgliederlisten für politisch aktive Vereine...

Man kann verschlüsselte Dokumente auch als Quick&Dirty Alternative zu verschlüsselten E-Mails verwenden, indem man den Inhalt in ein verschlüsseltes Dokument schreibt und deses Dokument als Anhang mit der E-Mail schickt. Das Passwort zum Öffnen des Dokumentes muss man dem Empfänger über einen sicheren Kanal mitteilen.

LibreOffice Dokumente

LibreOffice bietet seit Version 3.5 die Möglichkeit, Dokumente mit AES256 verschlüsselt zu speichern. Dafür muss man Eigenschaften Dialog der Datei auf dem Reiter *Sicherheit* das Dokument mit einem Passwort schützen (Abb. 13.1)

Um keine Spuren auf der Festplatte zu hinterlassen, sollte man den Schutz aktivieren, bevor das Dokument erstmalig gespeichert wird und bevor sensitive Daten in das Dokument geschrieben werden. Der Schutz funktioniert für Textdokumente, Tabellen usw.

PDF Dokumente

Der PDF-Standard definiert ein Berechtigungsmodell mit abgestuften Rechten für Aktionen wie Drucken erlauben, Modifikationen erlauben... Wenn man ein Passwort für das Öffnen des Dokumentes vergibt, dann wird das Dokument verschlüsselt gespeichert. Dabei kommen in Abhängigkeit von der PDF Version folgende Cipher zum Einsatz:

1. PDF v1.4: RC4 40-128 Bit (sehr schwache Verschlüsselung)
2. PDF v1.5: Public Key Cryptography Standard PKCS#7 mit SHA
3. PDF v1.6: AES128, PKCS#7 mit SHA256
4. PDF v1.7-extension-level-3: AES256
5. PDF v1.7-extension-level-8: AES256 mit mehreren Passwörtern

LibreOffice und OpenOffice.org bieten die Möglichkeit, beim PDF-Export ein Passwort für das Öffnen der PDF-Datei festzulegen. Die beiden Office-Suiten exportieren PDF-Dokumente in PDF v1.4. Demzufolge werden die exportierten PDF Dateien nur mit RC4 verschlüsselt. Adobe Acrobat unterstützt die aktuellste Version. Wenn man die Sicherheit des Schutzes einschätzen möchte, muss man sich also darüber informieren, in welcher PDF Version der PDF Export erfolgt.

Einige Crypto-Gurus haben uns darauf hingewiesen, dass es viele Tools geben soll, die angeblich die Verschlüsselung von PDF-Dokumenten auf Knopfdruck entfernen können (*PDF Password Remover*, *PDF Passwort Knacker* u.a.m.)

> *Sie können Ihre eigene PDF Datei nicht mehr drucken oder kopieren? Kein Problem! Mit PDF Passwort Knacker entfernen Sie die PDF Verschlüsselung spielend einfach per Knopfdruck. (Werbetext)*

Man muss die Werbung der Tools schon sehr genau lesen, um zu erkennen, dass diese Tools die Verschlüsselung nicht auf Knopfdruck entfernen können, wenn das Öffnen des PDF Dokumentes ein Passwort erfordert. Dann sind diese PDF Passwort Knacker hilflos, weil das komplette Dokument verschlüsselt ist. Einige Tools bieten dann die Möglichkeit, einen Brute Force Angriff auf das Passwort zu starten, was je nach Stärke des Passwortes einige tausend Jahre dauern kann.

13.4 Quick and Dirty mit GnuPG

Eine Möglichkeit ist die Verschlüsselung einzelner Dateien mit GnuPG oder PGP. Einfach im bevorzugten Dateimanager mit der rechten Maustaste auf eine Datei klicken und den Menüpunkt *Datei verschlüsseln* wählen. Mit der Auswahl eines Schlüssels legt man fest, wer die Datei wieder entschlüsseln kann. Für Backups wird in der Regel der eigene Schlüssel verwendet. Es ist auch möglich, mehrere Schlüssel für verschiedene Empfänger zu nutzen. Die Verwaltung der OpenPGP Schlüssel ist im Kapitel *E-Mails verschlüsseln* beschrieben. Anschließend ist das unverschlüsselte Orginal NICHT(!) in den

Papierkorb sondern in den Reißwolf zu werfen.

Sollen mehrere Dateien in einem Container verschlüsselt werden, erstellt man ein Verzeichnis und kopiert die Dateien dort hinein. Anschließend verpackt man dieses Verzeichnis mit *WinZip, 7zip* oder anderen Tools in ein Archiv und verschlüsselt dieses Archiv.

Wird die Option *Symmetrisch verschlüsseln* gewählt, erfolgt die Verschlüsselung nicht mit einem Schlüssel sondern nur mit einer Passphrase. Die Entschlüsselung erfordert dann ebenfalls nur die Angabe dieser Passphrase und keinen Key. Diese Variante wird für Backups empfohlen, die man auch nach einem Crash bei totalem Verlust aller Schlüssel wieder herstellen will.

Zum Entschlüsseln reicht in der Regel ein Klick (oder Doppelklick) auf die verschlüsselte Datei. Nach Abfrage der Passphrase für den Schlüssel liegt das entschlüsselte Orginal wieder auf der Platte.

13.4.1 GnuPG für WINDOWS

Diese simple Verschlüsselung klappt allerdings unter WINDOWS nicht auf Anhieb. Es ist zuerst die nötige Software zu installieren. Folgende Varianten kann man probieren:

1. Das Programmpaket **gpg4win** enthält eine Erweiterung für den Windows Explorer, die zusätzliche Menüpunkte im Kontextmenü einer Datei bzw. Verzeichnisses einfügt.

   Download: http://www.gpg4win.org

2. Für Nutzer, die es gern etwas einfacher und übersichtlicher mögen, gibt es die Tools **gpg4usb** http://gpg4usb.cpunk.de oder **Portable PGP** http://ppgp.sourceforge.net (eine Java-App). Diese kleinen Tools können Texte und Dateien ver- bzw. entschlüsseln und sind auch USB-tauglich. Sie können auf einem USB-Stick mitgenommen werden. Sie speichern die OpenPGP-Keys auf dem Stick und integrieren sich nicht in den Explorer.

13.5 dm-crypt für Linux

dm-crypt ist seit Version 2.6.4 fester Bestandteil des Linux-Kernels und somit in allen aktuellen Distributionen enthalten. Es nutzt den Device-Mapper. Folgende Software wird außerdem benötigt:

- Das Tool **cryptsetup** (mit LUKS-Support) kann zum Erstellen, Öffnen und Schließen der verschlüsselten Container eingesetzt werden. Aktuelle Distributionen enthalten es: Debian GNU/Linux im Packet *cryptsetup*, SuSE-Linux im Packet *util-linux-crypto*.

  Einige Distributionen installieren das Tool unter dem Namen *cryptsetup-luks*. Die im Folgenden beschriebenen Befehle sind dann entsprechend anzupassen. Besser wäre es, einen Link zu erstellen. Dann funktionieren auch die Scripte *mount.crypt* und *umount.crypt* aus der Sammlung pam-mount.

  ```
  # ln -s /usr/sbin/cryptsetup-luks /sbin/cryptsetup
  ```

- Das Packet **pmount** enthält einen Wrapper für das *mount*-Kommando, welcher automatisch verschlüsselte Laufwerke erkennt und vor dem Einbinden das Passwort abfragt. Aktuelle Debian-Distributionen verwenden es standardmäßig.

- Die Sammlung **pam-mount** enthält weitere Scripte, die das Öffnen und Schließen verschlüsselter Container vereinfachen. Die Scripte ermöglichen beispielsweise das Öffnen eines Containers automatisch beim Login. Unter Debian installiert man die Tools wie üblich mit

  ```
  # aptitude install libpam-mount.
  ```

- Das Kernelmodul **dm_crypt** muss vor der Verwendung der oben genannten Scripte geladen werden. In Abhängigkeit von der bevorzugten Distribution und der Installationsvariante wird das Modul bereits beim Booten geladen oder ist statisch in *initrd.img* eingebunden. Einfach probieren.

  Sollte beim Erstellen oder Öffnen eines verschlüsselten Containers die folgende Fehlermeldung auftreten:

  ```
  Command failed: Failed to setup dm-crypt key mapping.
  Check kernel for support for the aes-cbc-essiv:sha256 cipher
  ```

  ist das Kernel-Modul *dm_crypt* zu laden:

  ```
  # modprobe dm_crypt
  ```

  Außerdem sollte das Modul in die Liste der beim Systemstart zu ladenden Module eingefügt werden. In der Datei */etc/modules* ist die Zeile *dm_crypt* anzuhängen.

13.5.1 Bis zu 8 Passwörter mit LUKS

Die LUKS-Erweiterung von *cryptsetup* erlaubt es, bis zu 8 Passphrasen und Keyfiles zum Öffnen eines Containers zu nutzen. Damit ist es möglich, mehreren Nutzern den Zugriff mit einem eigenen Passwort zu erlauben.

Soll ein verschlüsselter Container mit dem Login eines Nutzers automatisch geöffnet werden, muss eines der 8 möglichen Passwörter mit dem Login-Passwort des Nutzers identisch sein. Login-Manager wie KDM oder GDM können das eingegebene Passwort an das pam-mount Modul weiterreichen. Dieses Feature kann beispielsweise für ein verschlüsseltes */home* Verzeichnis genutzt werden.

WICHTIG: bei Änderung des Login-Passwortes muss auch das Paswort für den Container geändert werden. Sie werden nicht automatisch synchronisiert.

13.5.2 Verschlüsselten Container erstellen

Alle folgenden Schritte sind als *root* auszuführen. Zum Aufwärmen soll zuerst die Partition */dev/hda4* verschlüsselt werden. Debian und Ubuntu enthalten das Skript luksformat, dass alle Aufgaben erledigt.

```
# luksformat -t ext3 /dev/hda4
```

Das ist alles. Der Vorgang dauert ein wenig und es wird 3x die Passphrase abgefragt. Ein Keyfile kann dieses Script nicht nutzen! Um einen USB-Stick komplett zu verschlüsseln, wählt man */dev/sdb1* oder */dev/sda1*. Es ist vor(!) Aufruf des Kommandos zu prüfen, unter welchem Device der Stick zur Verfügung steht.

Verschlüsselten Container erstellen für Genießer

Am Beispiel einer verschlüsselten Containerdatei werden die einzelnen Schritte beschrieben, welche das Script *luksformat* aufruft. Soll eine Partition (Festplatte oder USB-Stick) verschlüsselt werden, entfallen die Schritte 1 und 8. Das als Beispiel genutzte Device */dev/loop5* ist durch die Partition zu ersetzen, beispielsweise */dev/hda5* oder */dev/sdb1*.

1. Zuerst ist eine leere Imagedatei zu erstellen. Im Beispiel wird es unter dem Dateinamen *geheim.luks* im aktuellen Verzeichnis erstellt. Der Parameter *count* legt die Größe in MByte fest. Anschließend ist das Image als Loop-Device einzubinden. Das Kommando *losetup -f* ermittelt das nächste freie Loop-Device (Ergebnis: *loop0*).

   ```
   # dd if=/dev/zero of=geheim.luks bs=1M count=100
   # losetup -f
   /dev/loop0
   # losetup /dev/loop0 geheim.luks
   ```

2. Die ersten 2 MByte sind mit Zufallswerten zu füllen. Das Füllen der gesamten Datei würde sehr lange dauern und ist nicht nötig:

```
# dd if=/dev/urandom of=/dev/loop0 bs=1M count=2
```

3. Anschließend erfolgt die LUKS-Formatierung mit der Festlegung der Verschlüsselung. Die Option -y veranlaßt eine doppelte Abfrage des Passwortes, das *keyfile* ist optional

```
# cryptsetup luksFormat -c aes-xts-plain64 -s 256 -h sha512
                        -y /dev/loop0 [ keyfile ]
```

4. Das verschlüsselte Device wird dem Device-Mapper unterstellt. Dabei wird das zuvor eingegebene Passwort abgefragt. Das Keyfile ist nur anzugeben, wenn es auch im vorherigen Schritt verwendet wurde. Der <name> kann frei gewählt werden. Unter /dev/mapper/<name> wird später auf den verschlüsselten Container zugegriffen:

```
# cryptsetup luksOpen /dev/loop0 <name> [ keyfile ]
```

5. Wer paranoid ist, kann das verschlüsselte Volume mit Zufallszahlen füllen. Der Vorgang kann in Abhängigkeit von der Größe der Containerdatei sehr lange dauern:

```
# dd if=/dev/urandom of=/dev/mapper/<name>
```

6. Ein Dateisystem wird auf dem Volume angelegt:

```
# mkfs.ext3 /dev/mapper/<name>
```

7. Das Volume ist nun vorbereitet und wird wieder geschlossen:

```
# cryptsetup luksClose <name>
```

8. Die Containerdatei wird ausgehängt:

```
# losetup -d /dev/loop0
```

13.5.3 Passwörter verwalten

Mit root-Rechten ist es möglich, bis zu 7 zusätzliche Passwörter für das Öffnen eines Containers festzulegen oder einzelne Passwörter wieder zu löschen.

Um die Passwörter einer verschlüsselten Imagedatei *geheim.img* zu verwalten, ist die Imagedatei zuerst als Loop-Device einzuhängen, beispielsweise als */dev/loop5*. Dieser Schritt entfällt für verschlüsselte Partitionen:

```
# losetup /dev/loop5 geheim.luks
```

Das Hinzufügen eines Passwortes und damit eines neuen Keyslots erfolgt mit folgendem Kommando, wobei als <device> beispielsweise */dev/loop5* für die eingebundene Imagedatei oder */dev/sda5* für eine Festplattenpartition anzugeben ist. Das Keyfile ist optional. Mit der Option –key-slot wählt man einen bestimmten Slot von 0...7 aus.

```
# cryptsetup --key-slot <slot>  luksAddKey <device> [ keyfile ]
```

Ein Keyslot und das zugehörige Passwort können mit folgendem Kommando wieder entfernt werden:

```
# cryptsetup luksKillSlot <device> <slot>
```

Als <slot> ist die Nummer des Keyslots anzugeben, eine Zahl von 0...7. Es ist also nötig, sich zu merken, welches Passwort auf welchen Keyslot gelegt wurde. Eine Übersicht, welche Keyslots belegt und welche noch frei sind, liefert *luksDump*:

```
# cryptsetup luksDump <device>
LUKS header information for <device>
...
Key Slot 0: DISABLED
Key Slot 1: ENABLED
     Iterations:
     Salt:

     Key material offset:
     AF stripes:
Key Slot 2: DISABLED
Key Slot 3: DISABLED
Key Slot 4: DISABLED
Key Slot 5: DISABLED
Key Slot 6: DISABLED
Key Slot 7: DISABLED
```

13.5.4 Verschlüsselten Container öffnen/schließen

Aktuelle Linux Distributionen erkennen verschlüsselte Partitionen auf Festplatten und USB-Sticks automatisch und fragen die Passphrase ab, sobald das Gerät erkannt und im Dateimanager geöffnet wird. Einfach Anschließen, im Dateimanager öffnen und auf den Passwort-Dialog wie im Bild 13.2 warten.

Abbildung 13.2: Passwort-Abfrage für verschlüsselten USB-Stick

Auf der Kommandozeile (mit Keyfile)

Um eine verschlüsselte Partition auf einem USB-Stick auf der Kommandozeile zu öffnen, sind zwei Schritte als *root* nötig.

1. Im ersten Schritt wird das verschlüsselte Device dem Device-Mapper zu unterstellt. Der *name* kann frei gewählt werden. Zusätzlich kann man ein Keyfile nutzen.

   ```
   > sudo cryptsetup open --type luks /dev/sdc1 <name> [keyfile]
   Enter LUKS passphrase:
   ```

2. Danach kann es mit mount in das Dateisystem eingehängt werden, z.B. nach /mnt.

   ```
   > sudo mount /dev/mapper/<name> /mnt
   ```

Das Schließen des Containers erfolgt in umgekehrter Reihenfolge. Dabei werden alle Keys für den Zugriff auf den Container im Kernel sicher gelöscht (wipe).

```
> sudo umount /mnt
> sudo cryptsetup close <name>
```

Containerdatei öffnen

Das Öffnen einer Containerdatei auf der Kommadozeile erfordert drei Schritte als *root*. Als erstes ist die verschlüsselte Imagedatei als Loop Device einzuhängen. Das Loop-Device kann dann wie eine verschlüsselte Partition behandelt werden.

```
> sudo losetup /dev/loop0 geheim.luks
> sudo cryptsetup open --type luks /dev/loop0 <name> [keyfile]
Enter LUKS passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Containers erfolgt in umgekehrter Reihenfolge.

```
> sudo umount /mnt
> sudo cryptsetup close <name>
> sudo losetup -d /dev/loop0
```

Truecrypt und Veracrypt Container öffnen

cryptsetup kann auch Truecrypt und Veracrypt Container öffnen. Auf einem aktuellen Linux System muss man also keine zusätzliche Software installieren, wenn man gelegentlich Truecrypt/Veracrypt Container öffnen möchte. Eine Truecrypt verschlüsselte Partition auf dem USB-Stick öffnet man in zwei Schritten:

```
> sudo cryptsetup [Optionen] open --type tcrypt /dev/sdc1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Als [Optionen] können zusätzlich folgende Parameter angegeben werden:

- - -veracrypt verwendet man für Container im Veracrypt Format.
- - -key-file kann man mehrfach nutzen, um Schlüsseldateien anzugeben.
- - -tcrypt-hidden öffnet den Hidden Container im Truecrypt Volume.
- - -tcrypt-system ist für Systempartionen mit Boot Manager zu nutzen.
- - -readonly muss man nicht erklären.

Wenn man eine Containerdatei öffnen möchte, dann ist die Datei zuerst als Loop Device einzuhängen. Das Loop-Device kann dann wie eine verschlüsselte Partition behandelt werden.

```
> sudo losetup /dev/loop1 geheim.tc
> sudo cryptsetup [Optionen] open --type tcrypt /dev/loop1 <name>
Enter passphrase:
> sudo mount /dev/mapper/<name> /mnt
```

Das Schließen des Container erfolgt wie oben bei LUKS.

Komfortabel beim Login

Mit Hilfe des Modules pam-mount ist es möglich, das Anmeldepasswort zu nutzen, um standardmäßig beim Login einen oder mehrere Container zu öffnen. Insbesondere für verschlüsselte /home Partitionen ist dies sinnvoll und komfortabel.

Folgende Konfigurationen sind für einen Crypto-Login anzupassen:

1. **PAM-Konfiguration:** Dem PAM-Dämon ist mitzuteilen, dass er das Modul *mount* zu verwenden hat und das Login-Passwort zu übergeben ist. Gut vorbereitete Distributionen wie Debian und aktuelle Ubuntu(s) benötigen nur einen Eintrag in den Dateien */etc/pam.d/login*, */etc/pam.d/kdm* und */etc/pam.d/gdm*:

   ```
   @include common-pammount
   ```

2. **pam-mount Modul:** Das Modul wird konfiguriert in der XML-Datei */etc/security/pam_mount.conf.xml*. Am Anfang der Datei findet man eine Section für Volumes, die beim Login geöffnet werden sollen. Im ersten Beispiel wird bei allen Logins die verschlüsselte Partition /dev/hda4 als /home eingebunden:

   ```
   <volume fstype="crypt" path="/dev/hda4" mountpoint="/home" />
   ```

   Das zweite Beispiel zeigt die Einbindung einer verschlüsselten Containerdatei /geheim.luks als HOME für den User Pitschie. Die Containerdatei wird nur geöffnet, wenn Pitschie sich anmeldet.

   ```
   <volume user="pitschie" fstype="crypt" path="/geheim.luks"
           mountpoint="/home/pitschie" options="loop" />
   ```

3. **fstab:** Da beim Booten keine Partition nach */home* gemountet werden soll, ist evtl. der entsprechende Eintrag in der Datei */etc/fstab* zu löschen.

13.5.5 Debian GNU/Linux komplett verschlüsseln

In einem komplett verschlüsselten Sytem sind sowohl die Daten als auch die Systemkonfiguration und Software verschlüsselt. Debian ab Version 4.0r1 (etch) bietet bereits beim Installieren die Option, ein komplett verschlüssltes System unter Ausnutzung der gesamten Festplatte zu installieren. Lediglich für */boot* bleibt ein kleiner unverschlüsselter Bereich.

Um diese einfache Variante zu nutzen, wählt man im Installations-Dialog *Festplatte partitionieren* die Option *Geführt - gesamte Platte mit verschlüsseltem LVM*. Im folgenden Schritt ist die Passphrase einzugeben, welche das System sichert. Diese Passphrase wird später bei jedem Bootvorgang abgefragt.

```
Partitionsmethode:

    Geführt - verwende vollständige Festplatte
    Geführt - gesamte Platte verwenden und LVM einrichten
  > Geführt - gesamte Platte mit verschlüsseltem LVM
    Manuell
```

Ein vollständig verschlüsseltes System macht es böswilligen Buben sehr schwer, bei einem *heimlichen Hausbesuch* die Software zu manipulieren und einen Trojaner zu installieren. Es ist jedoch nicht unmöglich. Wer noch einen Schritt weiter gehen will, erstellt nach der Installation eine bootfähige CD-ROM mit einer Kopie des sauberen Verzeichnis */boot* und bootet in Zukunft immer von der CD. (Oder man geht zum Psychiater und lässt seine Paranoia behandeln.)

Man sollte nicht aus Zeitgründen auf ein Überschreiben der alten Daten mit Zufallszahlen verzichten. Um die Position verschlüsselter Daten auf der Platte zu verstecken und Daten der alten Installation zu vernichten, bietet die Installationsroutine die Option, den Datenträger mit Zufallszahlen zu überschreiben. Das dauert zwar einige Zeit, ist aber ein sinnvolles Feature.

13.5.6 Ubuntu komplett verschlüsseln

Mit der Version Ubuntu 12.10. ist es nicht mehr nötig, die alternate desktop cd von Ubuntu zu nutzen. Auf Wunsch der EFF.org haben die Entwickler die Full Disc Encryption in den Installer der Desktop-Version integriert. Man kann bei einer **Neuinstallation** nach Auswahl der Sprache im zweiten Schritt die Komplettverschlüsselung der Festplatte aktivieren.

13.5.7 HOME-Verzeichnis verschlüsseln

Die Verschlüsselung der persönlichen Daten im $HOME-Verzeichnis bieten alle Linux-Distributionen bei der Installation an. Wer keine Komplettverschlüsselung nutzen möchte, sollte zumindest diese Option aktivieren. Der Container mit den verschlüsselten Daten wird beim Login automatisch geöffnet. Die Nutzung ist vollständig transparent. Bei Verlust des Laptops sind die Daten jedoch geschützt.

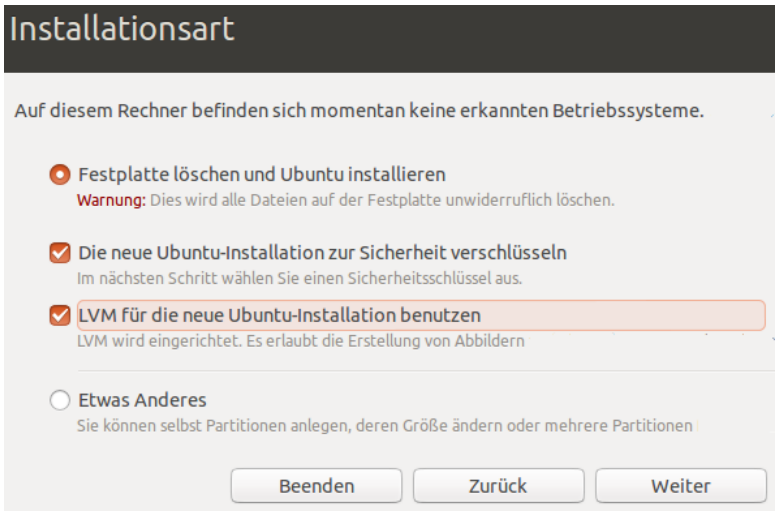


Abbildung 13.3: Full Disk Encryption bei der Installation von Ubuntu wählen

13.5.8 SWAP und /tmp verschlüsseln

Das */tmp*-Verzeichnis und der SWAP Bereich können unter Umständen persönliche Informationen enthalten, die im Verlauf der Arbeit ausgelagert wurden. Wenn eine komplette Verschlüsselung des Systems nicht möglich ist, sollte man verhindern, das lesbare Datenrückstände in diesen Bereichen verbleiben.

Das Verzeichnis */tmp* kann man im RAM des Rechners ablegen, wenn dieser hinreichend groß dimensioniert ist. Mit dem Ausschalten des Rechners sind alle Daten verloren. Um diese Variante zu realisieren bootet man den Rechner im abgesicherten Mode, beendet die grafische Oberfläche (X-Server) und löscht alle Dateien in */tmp*. In der Datei */etc/fstab* wird folgender Eintrag ergänzt:

```
tmpfs  /tmp  tmpfs    defaults,size=256m   0 0
```

Die Bereiche SWAP und */tmp* können im Bootprozess als verschlüsselte Partitionen mit einem zufälligen Passwort initialisiert und eingebunden werden. Mit dem Ausschalten des Rechners ist das Passwort verloren und ein Zugriff auf diese Daten nicht mehr möglich.

Achtung: Suspend-to-RAM und Suspend-to-Disk funtionieren mit einer verschlüsselten SWAP-Partition noch nicht.

Debian GNU/Linux

Debian und Ubuntu enthalten ein Init-Script, welches eine einfache Verschlüsselung von SWAP und */tmp* ermöglicht, wenn diese auf einer eigenen Partition liegen.

In der Datei */etc/crypttab* sind die folgenden Zeilen einzufügen, wobei */dev/hda5* und */dev/hda8* durch die jeweils genutzten Partitionen zu ersetzen sind:

cryptswp	/dev/hda5	/dev/urandom	swap
crypttmp	/dev/hda8	/dev/urandom	tmp

In der Datei */etc/fstab* sind die Einträge für swap und /tmp anzupassen:

/dev/mapper/cryptswp	none	swap	sw	0 0
/dev/mapper/crypttmp	/tmp	ext2	defaults	0 0

Anschließend ist der Rechner neu zu booten und beide Partitionen sind verschlüsselt.

Achtung: Die Partition für */tmp* darf kein Dateisystem enthalten! Soll eine bereits verwendete */tmp*-Partionion verschlüsselt werden, ist diese erst einmal nach dem Beenden des X-Servers(!) zu dismounten und zu überschreiben:

```
# umount /tmp
# dd if=/dev/zero of=/dev/hda8
```

13.6 Backups verschlüsseln

Es ist beruhigend, wenn alles Nötige für eine komplette Neuinstallation des Rechners zur Verfügung steht: Betriebssystem, Software und ein Backup der persönlichen Daten. Betriebssystem und Software hat man als Linux-Nutzer mit einer Installations-CD/DVD der genutzen Distribution und evtl. einer zweiten CD für Download-Stuff schnell beisammen. Für WINDOWS wächst in kurzer Zeit eine umfangreiche Sammlung von Software.

Für das Backup der persönlichen Daten habe ich eine kleine Ideensammlung zusammengestellt, die keinen Anspruch auf Vollständigkeit erhebt. Grundsätzlich sollten diese Daten verschlüsselt werden. Als Schlüssel für den Zugriff sollte eine gut merkbare Passphrase genutzt werden. Keyfiles oder OpenPGP-Schlüssel könnten bei einem Crash verloren gehen.

1. Die persönlichen Daten oder einzelne Verzeichnisse mit häufig geänderten Dateien könnte man regelmäßig mit einer Kopie auf einem verschlüsselten Datenträger synchronisieren (USB-Stick, externe Festplatte). Da nur Änderungen übertragen werden müssen, geht es relativ schnell.

2. Einzelne, in sich geschlossene Projekte könnten platzsparend als komprimiertes verschlüsseltes Archiv auf einem externen Datenträger abgelegt werden.

3. Größere abgeschlossene Projekte könnten auf einem optischen Datenträger dauerhaft archiviert werden.

13.6.1 Schnell mal auf den USB-Stick

Inzwischen gibt es preiswerte USB-Sticks mit beachtlicher Kapazität. Aufgrund der einfachen Verwendung sind sie für Backups im privaten Bereich gut geeignet. Für große Datenmengen kann man auch eine externe USB-Festplatte nutzen. Wer eine Beschlagnahme der Backupmedien befürchtet, findet vielleicht eine Anregung bei true-random[6].

Das Backupmedium sollte man mit Veracrypt oder DM-Crypt komplett verschlüsseln. Die vollständige Verschlüsselung verhindert eine Manipulation des Datenträgers. Der Verfassungsschutz demonstrierte auf der CeBIT 2007, dass sich mit manipulierten Sticks Trojaner einschleusen lassen. Die vollständige Verschlüsselung des Backup Mediums macht es überflüssig, sich um eine zusätzliche Verschlüsselung der Daten beim Backup zu kümmern. Man kann die Daten nach dem Öffnen des Backup Containers einfach synchronisieren.

Die von verschiedenen Herstellern angebotenen Verschlüsselungen sind oft unsicher. USB-Datentresore mit Fingerabdruckscanner lassen sich einfach öffnen[7]. Viele USB-Sticks mit Verschlüsselung verwenden zwar starke Algorithmen (in der Regel AES256), legen aber einen zweiten Schlüssel zur Sicherheit

[6] http://true-random.com/homepage/projects/usbsticks/small.html
[7] http://heise.de/-270060

auf dem Stick ab, der mit geeigneten Tools ausgelesen werden kann und Zugriff auf die Daten ermöglicht. Selbst eine Zertifizierung des NIST ist keine Garantie für eine saubere Implementierung, wie ein Artikel bei Heise [8] zeigt.

Unison-GTK

Für die Synchronisation der Daten steht z.B. Unison-GTK [9] für verschiedene Betriebssysteme (auch WINDOWS) zur Verfügung und bietet ein GUI für die Synchronisation. Die Installation ist einfach: Download, Entpacken und Binary starten. Linuxer können das Paket *unison-gtk* mit der Paketverwaltung installieren.

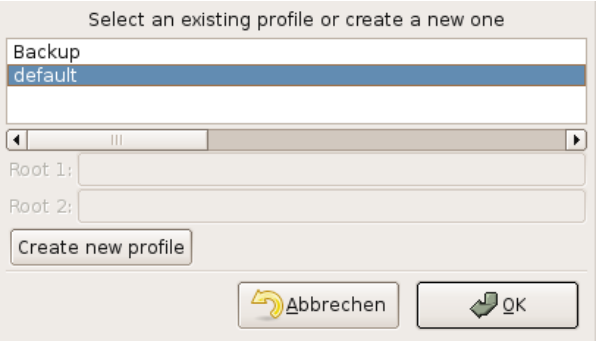


Abbildung 13.4: Profil nach dem Start von Unison-GTK auswählen

Nach dem ersten Start wählt man Quell- und Zielverzeichnis für das Default-Profil. Es ist möglich, mehrere Profile anzulegen. Bei jedem weiteren Start erscheint zuerst ein Dialog zur Auswahl des Profiles (Bild 13.4).

Nach Auswahl des Profiles analysiert Unison die Differenzen und zeigt im Haupfenster an, welche Aktionen das Programm ausführen würde. Ein Klick auf *Go* startet die Synchronisation.

Achtung: Unison synchronisiert in beide Richtungen und eignet sich damit auch zum Synchronisieren zweier Rechner. Verwendet man einen neuen (leeren) Stick, muss auch ein neues Profil angelegt werden! Es werden sonst alle Daten in den Quellverzeichnissen gelöscht, die im Backup nicht mehr vorhanden sind.

Neben der Möglichkeit, lokale Verzeichnisse zu synchronisieren, kann Unison auch ein Backup auf einem anderen Rechner via FTP oder SSH synchronisieren.

[8] http://heise.de/-894962
[9] http://www.cis.upenn.edu/ bcpierce/unison/

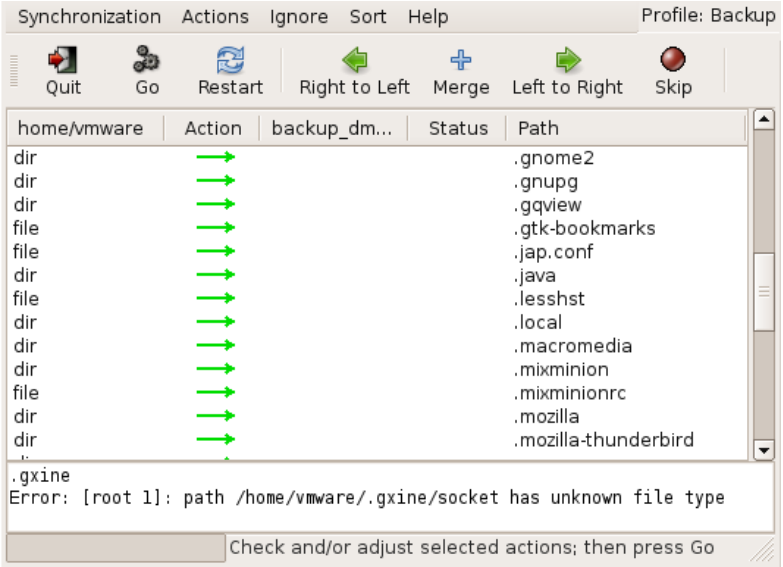


Abbildung 13.5: Hauptfenster von Unison-GTK

rsync

Das Tool *rsync* ist in allen Linux-Distributionen enthalten und insbesondere für Scripte einfach verwendbar. Es synchronisiert die Dateien eines Zielverzeichnisses mit dem Quellverzeichnis und überträgt dabei nur die Änderungen. Ein Beispiel zeigt das Sichern der E-Mails und Adressbücher von Thunderbird:

```
rsync -av --delete $HOME/.thunderbird /backup_dir/.thunderbird
```

Eine zweite Variante zum Sichern des gesamten $HOME inklusive der versteckten Dateien und exklusive eines Verzeichnisses (mp3) mit großen Datenmengen:

```
rsync -av --delete --include=$HOME/. --exclude=$HOME/mp3 $HOME /backup_dir/
```

Die Option *–delete* löscht im Orginal nicht mehr vorhandene Dateien auch in der Sicherungskopie. Weitere Hinweise liefert die Manualpage von rsync.

Standardmäßig sichert rsync keine versteckten Dateien und Verzeichnisse, die mit einem Punkt beginnen. Diese Dateien und Verzeichnisse müssen mit einem *–include* angegeben werden. Im Beispiel werden alle versteckten Verzeichnisse und Dateien mit gesichert.

Ein kleines Script, welches alle nötigen Verzeichnisse synchronisiert, ist schnell gestrickt. Eine backup-freundliche Struktur im $HOME-Verzeichnis erleichtert dies zusätzlich.

Grsync

GRsync ist ein grafischen Interface für rsync. Auch dieses Tool ist in allen Linux/Unix Distributionen enthalten.

Nach dem Start kann man mit dem Button "+" mehrere Profile für verschiedene, wiederkehrende Aufgaben anlegen. Jedem Profil wird ein Quell - und ein Zielverzeichnis sowei die rsync-Parameter zugeordnet. Ein Klick auf die kleine Rakete oben rechts startet die Synchronisation (Bild 13.6).

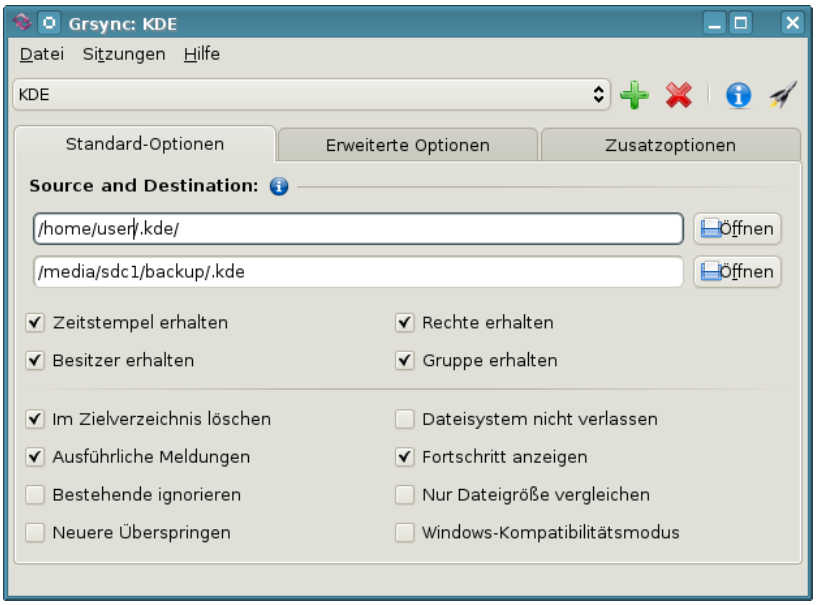


Abbildung 13.6: Hauptfenster von Grsync

13.6.2 Online Backups

Neben dem Backup auf einem externen Datenträger kann man auch Online-Speicher nutzen. Bei TeamDrive.com, DataStorageUnit.com, ADrive.com, rsync.net u.v.a.m. gibt es Angebote ab 3,- Euro monatlich. Wer einen eigenen (V)Server gemietet hat, kann seine Backups auch dort ablegen. Um die Verschlüsselung der Daten vor dem Upload muss man sich immer selbst kümmern.

Ein Online-Backup ist praktisch, wenn man mit Laptop in ein Land wie die USA reist. Bei der Einreise werden möglicherweise die Daten der Laptops gescannt und auch kopiert. Die EFF.org empfiehlt, vor der Reise die Festplatte zu "reinigen" [10]. Man könnte ein Online-Backup erstellen und auf dem eigenen Rechner die Daten sicher(!) löschen, also *shred* bzw. *wipe* nutzen. Bei Bedarf holt man sich die Daten wieder auf den Laptop. Vor der Abreise wird

[10] https://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t

das Online-Backup aktualisiert und lokal wieder alles gelöscht.

Mit dem Gesetzentwurf zum Zugriff auf Bestandsdaten der Telekommunikation (BR-Drs. 664/12) vom 24.10.2012 räumt die Bundesregierung den Geheimdiensten und Strafverfolgern die Möglichkeit ein, ohne richterliche Prüfung die Zugangsdaten zum Online-Speicher vom Provider zu verlangen. Um die gespeicherten Daten, die meist aus dem Bereich *privater Lebensführung* stammen, angemessen vor dem Verfassungsschutz zu schützen, ist man auf Selbsthilfe und Verschlüsselung angewiesen.

An ein Online-Backup werden deshalb folgende Anforderungen gestellt:

- Das Backup muss auf dem eigenen Rechner ver- und entschlüsselt werden, um die Vertraulichkeit zu gewährleisten.
- Es sollten nur geänderte Daten übertragen werden, um Zeitbedarf und Traffic auf ein erträgliches Maß zu reduzieren.

duplicity ist ein kleines Backuptool für Linux, dass die Daten lokal ver- und entschlüsselt, bevor sie in einen beliebigen Cloud-Speicher hochgeladen werden. Für die unverschlüsselten Cloud-Speicher kann man Verzeichnisse transparent mit *Boxcryptor*[11] oder *Cryptomator*[12] verschlüsseln. Beide gibt es für Windows, MacOS, Linux und diverse Smartphones.

E. Snowden hat in Interviews mehrfach vor Dropbox, Facebook und Google gewarnt und den amerikanischen Cloud-Provider Spideroak empfohlen, weil dieser Cloud-Provider die Daten irgendwie verschlüsselt. E. Snowden weiß aber nicht genau, wie Spideroak die Daten verschlüsselt. Hmmm - ein US-amerikanischer Provider, der die Daten irgendwie verschlüsselt. Ist das als Empfehlung ausreichend? Nein - für uns reicht es nicht.

Duplicity für Linux

Duplicity ist ein Backuptool für Linux/Unix speziell für die Nutzung von Online-Speicherplatz. Es bietet transparente Ver- und Entschlüsselung mit OpenPGP und überträgt nur geänderte Daten, um Traffic und Zeitbedarf minimal zu halten.

Debian und Ubuntu stellen in der Regel alles Nötige für die Installation in den Repositories bereit. *aptitude* spült es auf die Platte:

```
> sudo aptitude install duplicity
```

Duplicity ist ein Kommandozeilen Tool. Ein verschlüsseltes Backup schiebt man mit folgendem Kommando auf den Server:

```
> duplicity Verzeichnis Backupaddresse
```

Vom lokalen Verzeichnis wird ein Backup erstellt, mit OpenPGP symmetrisch verschlüsselt und unter der Backup Adresse abgelegt. Ein vorhandenes

[11] https://www.boxcryptor.com
[12] https://cryptomator.org

Backup wird aktualisiert. Das Passwort für die Verschlüsselung wird entweder beim Start des Programms abgefragt oder es wird die Environment Variable $PASSPHRASE verwendet. Um das Backup mit cron zu automatisieren, kann man ein kleines Shellscript schreiben:

```
#!/bin/sh
PASSPHRASE="gutes_passwort"
duplicity Verzeichnis Backupaddresse
```

Möchte man statt der symmetrischen Verschlüsselung einen OpenPGP-Key nutzen, verwendet man die Option *–encrypt-key* mit der ID oder Mail-Adresse des OpenPGP Key. Diese Option kann mehrfach angegeben werden, um mehreren Teilnehmern ein Restore des Backups zu erlauben.

```
> duplicity --encrypt-key="0x12345670" Verzeichnis Backupaddresse
```

Die **BackupAdresse** kodiert das Übertragungsprotokoll, den Server und das Verzeichnis auf dem Server. Duplicity kann mit vielen Protokollen umgehen. BackupAdressen haben folgenden Aufbau:

- Alle Anbieter von Online-Speicherplatz unterstützen webdav oder die SSL-verschlüsselte Übertragung mit webdavs:

  ```
  webdavs://user[:password]@server.tld/dir
  ```

- Amazon S3 cloud services werden unterstützt:

  ```
  s3://server/bucket_name[/prefix]
  ```

- Man kann sein IMAP-Postfach für das Backup nutzen, möglichst mit SSL-verschlüsselter Verbindung. Diese Variante ist nicht sehr performant viele Mail-Provider sehen das nicht gern:

  ```
  imaps://user[:password]@mail.server.tld
  ```

- Das sftp-Protokoll (ssh) ist vor allem für eigene Server interessant. Loginname und Passwort werden ebenfalls in der Adresse kodiert. Statt Passwort sollte man besser einen SSH-Key nutzen und den Key mit ssh-add vorher freischalten.

  ```
  ssh://user[:password]@server.tld[:port]/dir
  ```

- scp und rsync können ebenfalls für die Übertragung zum Server genutzt werden:

  ```
  scp://user[:password]@server.tld[:port]/dir
  rsync://user[:password]@server.tld[:port]/dir
  ```

  Das Verzeichnis ist bei rsync relativ zum Login-Verzeichnis. Um einen absoluten Pfad auf dem Server anzugeben, schreibt man 2 Slash, also //dir.

Ein **Restore** erfolgt nur in ein leeres Verzeichnis! Es ist ein neues Verzeichnis zu erstellen. Beim Aufruf zur Wiederherstellung der Daten sind Backupadresse und lokales Verzeichnis zu tauschen. Weitere Parameter sind nicht nötig.

```
> mkdir /home/user/restore
> duplicity Backupaddresse /home/user/restore
```

Weitere Informationen findet man in der manual page von *duplicity*.

Kapitel 14

Daten löschen

Neben der sicheren Aufbewahrung von Daten steht man gelegentlich auch vor dem Problem, Dateien gründlich vom Datenträger zu putzen. Es gibt verschiedene Varianten, Datein vom Datenträger zu entfernen. Über die Arbeit der einzelnen Varianten sollte Klarheit bestehen, anderenfalls erlebt man evtl. eine böse Überraschung.

14.1 Dateien in den Papierkorb werfen

Unter WIN wird diese Variante als *Datei(en) löschen* bezeichnet, was etaws irreführend ist. Es wird überhaupt nichts beseitigt. Die Dateien werden in ein spezielles Verzeichnis verschoben. Sie können jederzeit wiederhergestellt werden. Das ist kein Bug, sondern ein Feature.

Auch beim Löschen der Dateien in dem speziellen Müll-Verzeichnis werden keine Inhalte beseitigt. Lediglich die von den Dateien belegten Bereiche auf dem Datenträger werden als "frei" gekennzeichnet. Falls sie nicht zufällig überschrieben werden, kann ein mittelmäßig begabter User sie wiederherstellen. Forensische Toolkits wie *Sleuthkit* unterstützen dabei. Sie bieten Werkzeuge, die den gesamten, als frei gekennzeichneten Bereich, eines Datenträgers nach Mustern durchsuchen können und Dateien aus den Fragmenten wieder zusammensetzen.

14.2 Dateien sicher löschen (Festplatten)

Um sensible Daten sicher vom Datenträger zu putzen, ist es nötig, sie vor dem Löschen zu überschreiben. Es gibt diverse Tools, die einzelne Dateien oder ganze Verzeichnisse shreddern können.

- Das GpgSX für Windows bietet als Erweiterung für den Explorer die Möglichkeit, Dateien und Verzeichnisse mit einem Mausklick sicher zu löschen: *"Wipe..."*
- Für WINDOWS gibt es AxCrypt (http://www.axantum.com/AxCrypt). Das kleine Tool zur Verschlüsselung und Löschung von Dateien inte-

griert sich in den Dateimanager und stellt zusätzliche Menüpunkte für das sichere Löschen von Dateien bzw. Verzeichnissen bereit.

- Unter Linux kann KGPG einen Reißwolf auf dem Desktop installieren. Dateien können per Drag-and-Drop aus dem Dateimanager auf das Symbol gezogen werden, um sie zu shreddern.
- Für Liebhaber der Kommandozeile gibt es *shred* und *wipe* für Linux. Einzelne Dateien kann man mit *shred* löschen:

  ```
  > shred -u dateiname
  ```

  Für Verzeichnisse kann man *wipe* nutzen. Das folgende Kommando überschreibt rekursiv (Option -r) alle Dateien in allen Unterverzeichnissen 4x (Option -q) und löscht anschließend das gesamte Verzeichnis.

  ```
  > wipe -rqf verzeichnis
  ```

  Standardmäßig (ohne die Option -q) überschreibt *wipe* die Daten 34x. Das dauert bei großen Dateien sehr lange und bringt keine zusätzliche Sicherheit.

  Btrfs soll das kommende neue Dateisystem für Linux werden und wird bereits bei einigen Server-Distributionen eingesetzt. Bei diesem Dateisystem funktionieren shred und wipe NICHT. Btrfs arbeitet nach dem Prinzip *Copy on Write*. Beim Überschreiben einer Datei werden die Daten zuerst als Kopie in einen neuen Bereich auf der Festplatte geschrieben, danach werden die Metadaten auf den neuen Bereich gesetzt. Ein gezieltes Überschreiben einzelner Dateien auf der Festplatte ist bei Btrfs nicht mehr möglich.

Auch bei diesen Varianten bleiben möglicherweise Spuren im Dateisystem zurück. Aktuelle Betriebssysteme verwenden ein Journaling Filesystem. Daten werden nicht nur in die Datei geschrieben, sondern auch in das Journal. Es gibt kein Tool für sicheres Löschen von Dateien, welches direkten Zugriff auf das Journal hat. Die Dateien selbst werden aber sicher gelöscht.

14.3 Dateireste nachträglich beseitigen

Mit Bleachbit [1] kann man die Festplatte nachträglich von Dateiresten säubern. Das Programm gibt es für Windows und Linux. Linuxer können es auch aus den Repositories installieren.

Nach der Installation ist Bleachbit als Adminstrator bzw. root zu starten und nur die Option *Free disk space* zu aktivieren (Bild 14.1). Außerdem ist in den Einstellungen ein schreibbares Verzeichnis auf jedem Datenträger zu wählen, der gesäubert werden soll. Anschließend startet man die Säuberung mit einem Klick auf den Button *Clean*.

[1] http://bleachbit.sourceforge.net/download

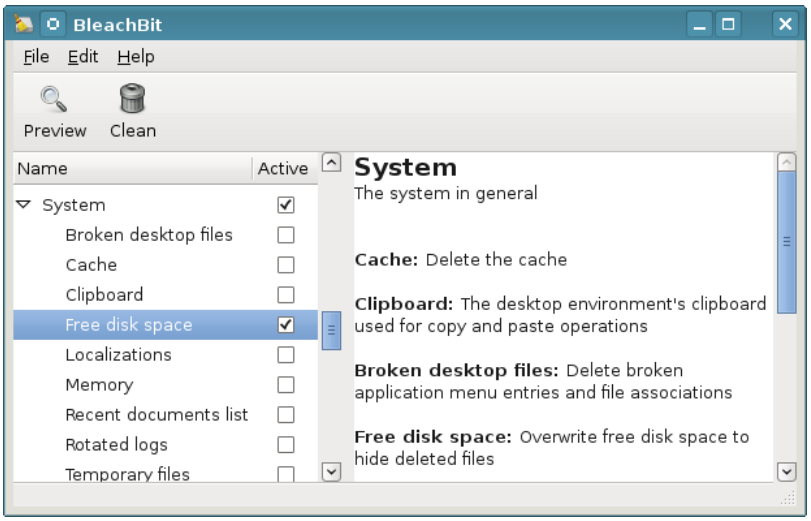


Abbildung 14.1: Bleachbit

Die Säuberung einer größeren Festplatte dauert einige Zeit. Dabei werden nur die als *frei* gekennzeichneten Bereiche überschrieben, das Dateisystem bleibt intakt.

14.4 Dateien sicher löschen (SSDs)

Alle oben genannten Tools für Festplatten funktionieren nicht mit Flash basierten Solid State Drives (SSD-Festpaltten und USB-Sticks)! Um die Speicherzellen zu schonen, sorgt die interne Steuerelektronik dafür, dass für jeden Schreibvorgang andere Zellen genutzt werden. Ein systematisches Überschreiben einzelner Dateien ist nicht möglich. Die Auswertung der Raw-Daten der Flash Chips ermöglicht eine Rekonstruktion mit forensischen Mitteln. Mehr Informationen liefert die Publikation *Erasing Data from Flash Drives* [2].

Für SSDs ist die Trim Funktion zu aktivieren. Dabei werden die Speicherzellen eines Blocks beim Löschen der Datei auf den Ursprungszustand zurück gesetzt. Zusätzliche Maßnahmen zum sicheren Löschen sind dann nicht mehr nötig. Die meisten aktuellen Betriebssystem aktivieren Trim nicht(!) standardmäßig. Folgende Schritte sind nötig, um Trim nach der Installation für SSDs zu aktivieren:

Windows 7 und neuer kann TRIM aktivieren. Starten sie das Programm *cmd* als Administrator, um ein Terminal zu öffnen. Im Terminal kann man mit folgendem Kommando den Status der Trim Funktion abfragen:

```
> fsutil behavior query disabledeletenotify
```

[2] http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf

Wenn ein Wert = 0 ausgegeben wird, ist Trim aktiviert. Wird ein Wert = 1 ausgegeben, aktivieren sie die Trim Funktion mit folgendem Kommando:

```
> fsutil behavior set disabledeletenotify 0
```

Linux unterstützt seit Kernel 2.6.33 die TRIM Funktions für SSDs. Das Dateisystem auf der SSD ist mit der Option discard zu mounten, um TRIM zu aktivieren.

- Für fest eingebaute Datenträger können die Optionen in der Datei /etc/fstab modifiziert und die Option discard eingefügt werden:

  ```
  UUID=[NUMS-LETTERS]  /  ext4  discard,errors=remount-ro  0 1
  ```

- Die mount-Optionen für USB-Sticks können mit usbmount angepasst werden. Nach der Installation des Paketes *usbmount* und *pmount* kann man in */etc/usbmount/usbmount.conf* die Mount-Optionen anpassen. Folgende Einstellungen funktionieren bei mir unter Ubuntu *precise*:

  ```
  MOUNTOPTIONS="discard,noexec,nodev,noatime,nodiratime"
  FS_MOUNTOPTIONS="-fstype=vfat,gid=floppy,dmask=0007,fmask=0117"
  ```

  Alle Nutzer, die unter Windows mit vFAT formatierte USB-Sticks einsetzen wollen, müssen zur Gruppe floppy gehören (was standardmäßig unter Ubuntu der Fall ist). Die vFAT formatierten Sticks müssen als root ausgehängt werden (mit *pumount*), bevor man den Stick abzieht. Anderenfalls kann es zu Datenverlusten kommen.

Ich werde für mich persönlich weiterhin die vollständige Verschlüsselung der USB-Sticks den Spielereien mit TRIM vorziehen. Damit werden nicht nur gelöschte Dateien geschützt sondern auch die noch vorhandenen Daten. Das Auslesen der RAW-Daten der Speicherzellen durch Forensiker ist dann ebenfalls wenig erfolgreich.

14.5 Gesamten Datenträger säubern (Festplatten)

Bevor ein Laptop oder Computer entsorgt oder weitergegeben wird, sollte man die Festplatte gründlich putzen. Am einfachsten erledigt man diesen Job mit Darik's Boot and Nuke (DBAN) [3] Live-CD. Nach dem Download ist das ISO-Image auf eine CD zu brennen und der Computer mit dieser CD zu booten. Es werden automatisch alle gefundenen Festplatten gelöscht - fertig.

Eine beliebige Linux Live-CD tut es auch (wenn man bereits eine Live-CD nutzt). Nach dem Booten des Live Systems öffnet man ein Terminal (Konsole) und überschreibt die gesamte Festplatte. Bei einem Aufruf wird der Datenträger 4x überschrieben, es dauert einige Zeit.

Für die erste IDE-Festplatte:

[3] http://www.dban.org/

```
> wipe -kq /dev/hda
```

Für SATA- und SCSI-Festplatte:

```
> wipe -kq /dev/sda
```

Wenn die Live-CD das Tool *wipe* nicht enthält, kann man alternativ *dd* (disk doubler) nutzen. Um die erste IDE-Festplatte einmal mit NULL und dann noch einmal mit Zufallszahlen zu überschreiben, kann man folgende Kommandos nutzen:

```
> dd if=/dev/zero of=/dev/hda
> dd if=/dev/urandom of=/dev/hda
```

(Einmal mit NULLEN überschreiben reicht, alles andere ist paranoid.)

14.6 Gesamten Datenträger säubern (SSDs)

Das komplette Löschen einer SSD-Platte oder eines USB-Sticks funktioniert am besten, wenn der Datenträger den ATA-Befehl SECURE-ERASE unterstützt. Diese Funktion muss allerdings durch den Datenträger bereitgestellt werden. Unter Linux kann man das Tool *hdparm* nutzen, um diese Funktion aufzurufen.

Als erstes ist zu prüfen, ob SECURE-ERASE unterstützt wird:

```
> sudo hdparm -I /dev/X
```

Das Ergebnis muss einen Abschnitt *Security* enthalten und muss auf *not frozen* stehen. Falls die Ausgabe *frozen* liefert, wird SECURE-ERASE im Bios des Rechners blockiert.

```
Security:
    Master password revision code = 64060
        supported
    not enabled
    not locked
    not frozen
        expired: security count
        supported: enhanced erase
```

Dann kann man ein Passwort setzen und den Datenträger vollständig löschen:

```
> sudo hdparm --user-master u --security-set-pass GEHEIM /dev/X
> sudo hdparm --user-master u --security-erase GEHEIM /dev/X
```

Falls der Datenträger SECURE-ERASE nicht unterstützt, bleibt nur das einfache Überschreiben des Datenträgers. Dabei werden aber nicht alle Speicherzellen garantiert gelöscht. Unter Linux auf der Kommandozeile wieder mit:

```
> dd if=/dev/zero of=/dev/sdc
```

Kapitel 15

Daten anonymisieren

Fotos, Office Dokumente, PDFs und andere Dateitypen enthalten in den Metadaten viele Informationen, die auf den ersten Blick nicht sichtbar sind, jedoch vieles verraten können.

- Fotos von Digitalkameras enthalten in den EXIF-Tags oft eine eindeutige ID der Kamera, Zeitstempel der Aufnahmen, bei neueren Modellen auch GPS-Daten. Die IPTC-Tags können Schlagwörter und Bildbeschreibungen der Fotoverwaltung enthalten. XMP Daten enthalten den Autor und der Comment üblicherweise die verwendete Software.

- Office Dokumente enthalten Informationen zum Autor, letzte Änderungen, verwendete Softwareversion und vieles mehr. Diese Angaben sind auch in PDFs enthalten, die mit der Export-Funktion von OpenOffice.org oder Microsoft Office erstellt wurden.

Vor dem Upload der Dateien ins Internet ist es ratsam, diese überflüssigen Informationen zu entfernen. Es gibt mehrere Firmen, die sich auf die Auswertung dieser Metadaten spezialisiert haben. Ein Beispiel ist die Firma Heypic, die die Fotos von Twitter durchsucht und anhand der GPS-Koordinaten auf einer Karte darstellt. Auch Strafverfolger nutzen diese Informationen. Das FBI konnte einen Hacker mit den GPS-Koordinaten im Foto seiner Freundin finden[1].

Der *StolenCameraFinder*[2] sucht anhand der KameraID in den EXIF-Daten alle Fotos, die mit dieser Digital-Kamera gemacht wurden (Smartphone Kameras werden nicht unterstützt). Da die Kamera ID mit hoher Wahrscheinlichkeit eindeutig einer Person zugeordnet werden kann, sind viele Anwendungen für diese Suche denkbar. Die verbesserte Version *CameraForensics*[3] ist nur für Strafverfolgung verfügbar.

[1] http://www.tech-review.de/include.php?path=content/news.php&contentid=14968
[2] http://www.stolencamerafinder.com
[3] https://www.cameraforensics.com

15.1 Fotos und Bilddateien anonymisieren

- **Irfan View** [4] (Windows) kann in Fotos mit *Öffnen* und *Speichern* die Metatags entfernen. Im Batchmode kann man die Funktion *Konvertieren* nutzen, um mehrere Bilder mit einem Durchgang zu bearbeiten. Man konvertiert die Fotos von JPEG nach JPEG und gibt dabei in den Optionen an, dass keine EXIF, XMP und IPTC Daten erhalten bleiben sollen.

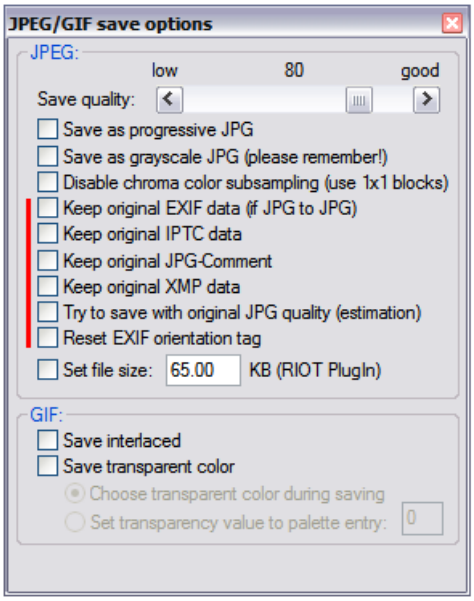


Abbildung 15.1: Informationen in Fotos löschen mit Irfan View

- **exiv2** (für Linux) ist ein nettes kleines Tool zum Bearbeiten von EXIF, XMP und IPTC Informationen in Bilddateien. Es ist in den meisten Linux Distributionen enthalten. Nach der Installation kann man z.B. Fotos auf der Kommandozeile säubern:

```
> exiv2 rm foto.jpg
```

15.2 PDF-Dokumente säubern

Für Windows gibt es das Tool **BeCyPDFMetaEdit** [5] in einer portablen Version für den USB-Stick oder als Installer. Nach dem Download und evtl. der Installation kann man das Tool starten und die zu säubernden PDF-Dokumente laden. Auf den Reitern *Metadaten* und *Metadaten (XMP)* klickt man auf den Button *Alle Felder löschen* und speichert das gesäuberte Dokument.

[4] http://www.heise.de/download/irfanview.html
[5] http://www.becyhome.de/download_ger.htm

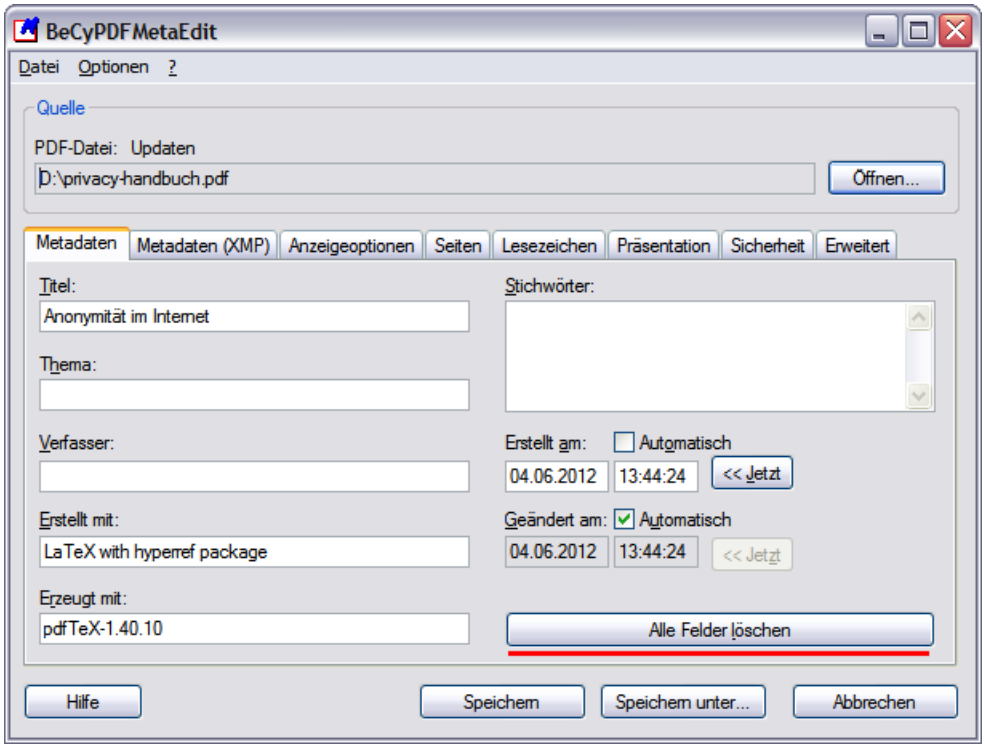


Abbildung 15.2: Metadaten in PDF-Dokumenten löschen

15.3 Metadata Anonymisation Toolkit (MAT) für Linux

Das Metadata Anonymisation Toolkit (MAT)[6] kann PNG und JPEG Bilder, PDF-Dokumente, Microsoft Office Dokumente, OpenOffice Dokumente, MP3 und FLAC Dateien säubern.

- PDF-Dokumente werden intern als Druckbild gerendert und aus dem Ergebnis wird ein neues Dokument erstellt. Formulare, Inhaltsverzeichniss, anklickbare Links usw. gehen dabei verloren.

  HINWEIS: Die eingebetteten Bilder in PDF-Dokumenten werden in MAT Version 0.6.x nicht mit gereinigt, dieses Feature ist für Version 0.7 geplant. Man muss beim Erstellen des PDFs darauf achten, dass die Bilder vorher gereinigt werden.

- Bei Office Dokumenten werden nur die Metadaten des Masterdokumentes gelöscht. Um evtl. eingebundene Bilder usw. muss man sich selbst kümmern. Am einfachsten benennt man das Dokument in eine ZIP-Datei um und behandelt es als Archiv.

[6] https://mat.boum.org/

- Archive werden entpackt, alle unterstützten Dateien werden gereinigt und das Archiv wird neu zusammengestellt. Man kann in den Einstellungen angeben, ob nicht unterstützte Dateien wieder ins Archiv gepackt werden sollen oder nicht.

Unter Debian, Ubuntu u.ä. installiert man MAT mit dem bevorzugten Paketmanager:

```
> sudo apt install mat
```

In der Programmgruppe *Zubehör* findet man den Starter für das GUI von MAT. Mit dem + kann man Dateien der Liste hinzufügen und mit dem Besen-Icon daneben säubern. Live-CDs sind eine Alternative, wenn man das Metadata Anonymisation Toolkit als Windows Anwender nutzen möchte. MAT ist in TAILS und in der JonDo Live-CD installiert.

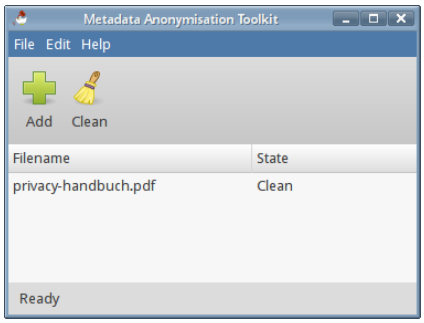


Abbildung 15.3: Dateien säubern mit MAT

Kapitel 16

Daten verstecken

Geheimdienste orakeln seit Jahren immer wieder, das *Terroristen* über versteckte Botschaften in Bildern kommunizieren. Telepolis berichtete 2001 und 2008 kritisch-ironisch über Meldungen von Scotland Yard, wonach islamische Terroristen ihre Kommunikation in pornografischen Bildern verstecken würden. Stichhaltige Belege für die Nutzung von **Steganografie** konnten bisher nicht geliefert werden. Andere Journalisten hinterfragten die Meldungen weniger kritisch:

"Bislang ist zwar noch nicht bewiesen, ob die Terrorverdächtigen die Bilder - bei einem Verdächtigen wurden 40.000 Stück gefunden - nur zum persönlichen Vergnügen heruntergeladen haben oder ob tatsächlich ein Kommunikationsnetzwerk aufgebaut wurde." (Welt Online[1], wieder einmal viel heiße Luft.)

Wie funktioniert diese Technik, über die Zeit Online bereits 1996 berichtete und können Nicht-Terroristen das auch nutzen?

Ein Beispiel

Statt Bits und Bytes werden in diesem Beispiel Buchstaben genutzt, um das Prinzip der Steganografie zu erläutern. Nehmen wir mal an, Terrorist A möchte an Terrorist B die folgende kurze Botschaft senden:

```
Morgen!
```

Statt die Nachricht zu verschlüsseln, was auffällig sein könnte, versteckt er sie in dem folgenden, harmlos aussehenden Satz:

```
Mein olles radio geht einfach nicht!
```

Wenn der Empfänger weiss, dass die eigentliche Botschaft in den Anfangsbuchstaben der Wörter kodiert ist, wäre es ganz gut, aber nicht optimal.

Ein Beobachter könnte auf den Gedanken kommen: *"Was - wieso Radio? Der zahlt doch keine GEZ!"* Er wird aufmerksam und mit ein wenig Probieren kann

[1] http://www.welt.de/politik/article2591337/

der die Botschaft extrahieren. Also wird Terrorist A die Nachricht zusätzlich verschlüsseln, nehmen wir mal eine einfache Caesar-Verschlüselung mit dem Codewort KAWUM, es entsteht:

```
Ilpcmg!
```

und ein neuer, halbwegs sinnvoller Satz wird konstruiert und verschickt.

16.1 Allgemeine Hinweise

Das Beispiel verdeutlicht, welche Voraussetzungen für die Nutzung von Steganografie zum Austausch von versteckten Botschaften gegeben sein müssen:

- Sender und Empfänger müssen sich darüber verständigt haben, wie die Nutzdaten versteckt werden.
- Das Passwort für die Verschlüsselung muss ausgetauscht werden.
- Die Modalitäten für den Austausch der Trägermedien müssen geklärt werden. Wo kann der Empfänger die Fotos mit den versteckten Botschaften finden?

Wenn diese Vorausetzungen geklärt sind, kann es losgehen

1. Der Absender schreibt seine Botschaft mit einem einfachen Texteditor.
2. Die Textdatei wird in einem (anonymisierten) Foto oder in einer Audiodatei mit Steganografie Tools wie z.B. *DIIT* oder *steghide* versteckt und gleichzeitig mit dem Passwort verschlüsselt.
3. Das Foto könnte man dem Empfänger per E-Mail senden. Das ist aber nicht unbedingt die beste Idee, da dabei die Metadaten der Kommunikation ausgewertet werden können (A hat B eine Mail geschrieben, Stichwort: Kommunikationsanalyse). Um auch die Metadaten der Kommunikation zu verstecken, könnte der Absender das Foto in seinem (anonymen) Blog veröffentlichen, man könnte es bei Flickr oder Twitpic hochladen oder an eine öffentliche Newsgruppe im Usenet senden. Wichtig ist, dass es öffentlich publiziert wird und der Empfänger nicht erkennbar ist. Außerdem kann der Absender verschiedene Maßnahmen ergreifen, um selbst anonym zu bleiben.
4. Der Empfänger muss wissen, wo er aktuelle Nachrichten finden kann. Fotos oder Audiodateien, in denen der Empfänger eine Botschaft vermutet, sind herunterzuladen.
5. Danach kann der Empfänger versuchen, die geheime Botschaft aus dem Trägermedium zu extrahieren. Dabei ist das gleiche Tool wie beim Verstecken zu verwenden. Wenn er alles richtig macht und das korrekte Passwort verwendet, wird die Textdatei extrahiert und kann mit einem einfachen Texteditor gelesen werden.

Unsichtbare Markierungen, Wasserzeichen

Man kann Steganografie Tools auch nutzen, um unsichtbare Wasserzeichen an Bildern oder Audiodateien anzubringen.

Wenn Fotos oder Videos nur einem kleinen Kreis von Personen zugänglich gemacht werden sollen, dann können individuelle Wasserzeichen steganografisch in den Dateien versteckt werden. Sollten diese Fotos oder Videos in der Öffentlichkeit auftauchen, kann das Leck anhand des unsichtbaren steganografischen Wasserzeichens ermittelt werden.

16.2 steghide

steghide ist ein Klassiker unter den Tools für Steganografie und wird auf der Kommandozeile gesteuert. Es kann beliebige Daten verschlüsselt in JPEG, BMP, WAV oder AU Dateien verstecken. Die verwendeten Algorithmen sind sehr robust gegen statistische Analysen. Die Downloadseite bietet neben den Sourcen auch Binärpakete für WINDOWS. Nutzer von Debian und Ubuntu installieren es wie üblich mit *aptitude*.

Um die Datei *geheim.txt* zu verschlüsseln und in dem Foto *bild.jpg* zu verstecken, ruft man es mit folgenden Parametern auf (mit dem Paramter -sf kann optional eine dritte Datei als Output verwendet werden, um das Original nicht zu modifizieren):

```
> steghide embed -cf bild.jpg -ef geheim.txt
Enter passphrase:
Re-Enter passphrase:
embedding "geheim.txt" in "bild.jpg"... done
```

Der Empfänger extrahiert die geheimnisvollen Daten mit folgendem Kommando (mit dem Parameter -xf könnte ein anderer Dateiname für die extrahierten Daten angegeben werden):

```
> steghide extract -sf bild.jpg
Enter passphrase:
wrote extracted data to "geheim.txt".
```

Außerdem kann man Informationen über die Coverdatei bzw. die Stegodatei abfragen. Insbesondere die Information über die Kapazität der Coverdatei ist interessant, um abschätzen zu können, ob die geheime Datei reinpasst:

```
> steghide info bild.jpg
     Format: jpeg
     Kapazität: 12,5 KB
```

16.3 stegdetect

Auch die Gegenseite ist nicht wehrlos. Manipulationen von steghide, F5, outguess, jphide usw. können z.B. mit *stegdetect* [2] erkannt werden. Ein GUI steht mit *xsteg* zur Verfügung, die Verschlüsselung der Nutzdaten kann mit *stegbreak* angegriffen werden. Beide Zusatzprogramme sind im Paket enthalten.

Der Name *stegdetect* ist eine Kurzform von *Steganografie Erkennung*. Das Programm ist nicht nur für den Nachweis der Nutzung von *steghide* geeignet, sondern erkennt anhand statistischer Analysen auch andere Tools.

Auch *stegdetect* ist ein Tool für die Kommandozeile. Neben der zu untersuchenden Datei kann mit einem Parameter -s die Sensitivität eingestellt werden. Standardmäßig arbeitet stegdetect mit einer Empfindlichkeit von 1.0 ziemlich oberflächlich. Sinnvolle Werte liegen bei 2.0...5.0.

```
> stegdetect -s 2.0 bild.jpg
F5(***)
```

Im Beispiel wird eine steganografische Manipulation erkannt und vermutet, dass diese mit dem dem Tool F5 eingebracht wurde (was nicht ganz richtig ist, da *steghide* verwendet wurde).

Frage: Was kann man tun, wenn auf der Festplatte eines mutmaßlichen Terroristen 40.000 Bilder rumliegen? Muss man jedes Bild einzeln prüfen?

Antwort: Ja - und das geht so:

1. Der professionelle Forensiker erstellt zuerst eine 1:1-Kopie der zu untersuchenden Festplatte und speichert das Image z.B. in *terroristen_hda.img*

2. Mit einem kurzen Dreizeiler scannt er alle 40.000 Bilder in dem Image:

   ```
   > losetup -o $((63*512)) /dev/loop0 terroristen_hda.img
   > mount -o ro,noatime,noexec /dev/loop0 /mnt
   > find /mnt -iname "*.jpg" -print0 | xargs -0 stegdetect -s 2.0 >> ergebnis.txt
   ```

   (Für Computer-Laien und WINDOWS-Nutzer sieht das vielleicht nach Voodoo aus, für einen Forensiker sind das jedoch Standardtools, deren Nutzung er aus dem Ärmel schüttelt.)

3. Nach einiger Zeit wirft man einen Blick in die Datei *ergebnis.txt* und weiß, ob es etwas interessantes auf der Festplatte des Terroristen gibt.

[2] http://www.outguess.org/download.php

Kapitel 17

Betriebssysteme

Der Widerstand gegen Ausforschung und Überwachung sowie der Kampf um die Hoheit über den eigenen Computer beginnt bei der Auswahl des Betriebssystems. Einige stichpunktartige Gedanken sollen zum Nachdenken anregen.

Windows

Mit Windows 8.0 hat Microsoft begonnen, dass bei Smartphones akzeptierte Device-based Tracking auch bei PCs einzuführen. Ähnlich wie Google bei Android will Microsoft als eine der größten Tracking Familien im Internet seine Datenberge erweitern und besser personalisieren.

Das Erstellen eines User-Account unter Windows 8.1 ist ein echtes Dark Pattern. Der Nutzer wird massiv gedrängt, den User-Account auf dem Rechner mit einem Online Konto bei Hotmail oder Windows Live zu verbinden. Nur wenn man in der Eingabemaske falsche Angaben macht, findet man in der Fehlermeldung den unscheinbaren Link für das Erstellen eines User-Account ohne Online Konto.

In Windows 10 wurde das Device-based Tracking weiter ausgebaut. Es wird für jeden Account auf dem Rechner eine *Unique Advertising ID* generiert. Diese ID wird auch Dritten zur eindeutigen Identifikation zur Verfügung gestellt. In der neuen Privacy Policy von Microsoft (Juli 2015) steht außerdem:

> *We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary ...*

Privaten Daten, die Microsoft in der Standardkonfiguration sammelt:

- Persönliche Interessen, die sich aus dem Surfverhalten ergeben sowie aus den per Apps gesammelten Daten werden an Microsoft gesendet (eine Sport-App sendet die bevorzugten Teams, eine Wetter-App die häufig angefragten Städte... usw.)

- Standortdaten aller Geräte mit Windows werden an MS übertragen. Es wird bevorzugt GPS oder die WLANs der Umgebung genutzt, um den Standort so genau wie möglich zu bestimmen.
- Kontaktdaten der Freunde und Bekannten werden an MS übertragen, wenn man Tools von Microsoft als Adressbuch nutzt.
- Inhalte von E-Mails, Instant Messages und Voice/Vidoe Messages (z.B Skype) gehören ebenfalls zu den den Daten, die MS sammelt.
- Der Windows Defender übermittelt alle installierten Anwendungen an Microsoft.
- Mit der digitalen Assistentin *Cortana* wird in der Standardkonfiguration eine Art Abhörzentrale eingerichtet, die das Wohnzimmer direkt mit Microsoft verbindet.
- Das Schreibverhalten wird analysiert und an Microsoft gesendet. Das Profil der typischen Tastenanschläge könnte zukünftig für die Identifikation bei Texteingaben in Webformularen oder Chats genutzt werden (Stichwort: Keystroke Biometrics[1]).
- Die eindeutige UUID, die Windows bei der Kommunikation mit Microsoftservern sendet (z.B. bei Softwareupdates), wird vom NSA und GCHQ als Selektor für Taylored Access Operations (TAO) verwendet, um gezielt die Computer von interessanten Personen oder Firmen anzugreifen. Microsoft ist seit 2007 Partner im PRISM Programm der NSA.
- Als besonderes Highlight gehören auch die automatisch generieten Recovery Keys der Festplattenverschlüsselung Bitlocker zu den Daten, die MS in seiner Cloud sammelt und NSA/FBI/CIA zur Verfügung stellt. (Crypto War 3.0?)

  Mit Windows 10 Pro oder Enterprise kann man den Upload des Recovery Key verhindern[2], indem man den Rechner einmal komplett verschlüsselt (mit Key Upload), dann die Verschlüsselung deaktiviert (damit muss das System wieder komplett entschlüsselt werden), den alten Recovery Schlüssel löscht und nochmal den Rechner komplett verschlüsselt. Erst beim zweiten Versuch wird man gefragt, ob man den Recovery Key evtl. lokal sichern möchte. Das kostet Zeit und ist auch wieder ein echtes Dark Pattern in der Benutzerführung.

Wenn man es schafft, einen Benutzeraccount ohne Cloud Anbindung einzurichten und in den Einstellungen unter Datenschutz die Privacy Features aktiviert, kann man die Sammelleidenschaft von Windows 10 etwas reduzieren aber nicht vollständig abstellen.[3]

---

[1] https://de.wikipedia.org/wiki/Tippverhalten/

[2] https://theintercept.com/2015/12/28/recently-bought-a-windows-computer-microsoft-probably-has-your-encryption-key/

[3] http://arstechnica.com/information-technology/2015/08/even-when-told-not-to-windows-10-just-cant-stop-talking-to-microsoft

Experten des BSI warnten 2013 vor dem Einsatz von Windows 8 in Kombination mit TPM 2.0 und bezeichneten es als inakzeptables Sicherheitsrisiko für Behörden und Firmen. Nutzer eines Trusted-Computing-Systems verlieren nach Ansicht der Experten die Kontrolle über ihren Computer. (Das ist doch der Sinn von Trusted Computing - oder?)

> *Aus Sicht des BSI geht der Einsatz von Windows 8 in Kombination mit einem TPM 2.0 mit einem Verlust an Kontrolle über das verwendete Betriebssystem und die eingesetzte Hardware einher. Daraus ergeben sich für die Anwender, speziell auch für die Bundesverwaltung und kritische Infrastrukturen, neue Risiken.*

T. Baumgärtner von Microsoft(!) erklärte in einer Antwort:

> *Das betrifft aber nur bestimmte Behörden, der Verfassungsschutz oder der BND sollten das System natürlich besser nicht nutzen.*
> ...
> *Für normale Nutzer bietet das TPM 2.0 ein enormes Plus an Sicherheit.*

Ähmm...

Virescanner sind Snakeoil

Für 90% der Windows Nutzer ist ein Virenscanner ein unverzichtbares Sicherheitstool aber nur 7% der Security Experten halten Virenscanner für sinnvoll. Warum sind Sicherheitsexperten so skeptisch und bezeichnen diese Produktgruppe als Schlangenöl?

1. Virenscanner sind eine komplexe Software, die immer wieder selbst schwere Fehler enthält, die von einem Angreifer ausgenutzt werden können. Insbesondere die Parser für komplexe, exotische Dateiformate enthalten immer wieder Fehler.[4] [5] [6] [7]

   Da ein Virescanner tief im System verankert ist und vollen Zugriff auf alle Systemkomponenten hat, kann ein Angreifer durch Ausnutzen von Bugs im Virenscanner das System vollständig kompromittieren ohne das der Anwender etwas bemerken kann.

   Außerdem wird die Implementierung von Sicherheitsfeatures durch Softwareentwickler (z.B. die konsequente Umsetzung von ASLR) durch Virenscanner behindert, wie der Ex-Firefox-Entwickler Robert O'Callahan berichtete. Er rät zur De-Installation.[8]

   Schlussfolgerung: Virenscanner machen den Rechner unsicher.[9]

[4] https://heise.de/-3250784
[5] https://heise.de/-3159436
[6] https://heise.de/-3149913
[7] https://heise.de/-2824437
[8] https://heise.de/-3609009
[9] https://www.golem.de/news/security-antivirenscanner-machen-rechner-unsicher-1407-108199.html

2. Viele Virenscanner brechen die TLS Transportverschlüsselung der Webbrowser und E-Mail Clients, um die verschlüsselten Inhalte zu scannen. Es ist ein klassischer man-in-the-middle Angriff mit Zustimmung der Anwender. Damit wird die Sicherheit der TLS Verschlüsselung massiv geschwächt.[10] [11]

   Moderne Webbrowser bieten umfangreiche Sicherheitsfeatures für TLS wie Strict Trasport Security (HSTS), Certificate Pinning (HKPS) oder mit Add-ons auch DANE/TLSA Validation. Virescanner beherrschen diese Sicherheitsfeatures in der Regel nicht. (Ich kenne kein Produkt der Schlangenöl Branche mit diesen Sicherheitsfunktionen.) Einige Virenscanner beherrschen nicht einmal das moderne TLS 1.2 und downgraden die Verschlüsselung auf die schwache Version TLS 1.0.

   AV-Hersteller sind grob fahrlässig bei HTTPS Interception.[12]

3. Mit der Installation eines Virescanners gibt der Nutzer praktisch die Hoheit über die Installation von Software teilweise auf. Es ist die Aufgabe eines Virenscanners, Software zu entfernen, die der Hersteller der Software für unpassend hält. Das kann auch zur Deinstallation von Software genutzt werden, die der Kunde nicht nutzen soll/darf.

4. In der Regel verwenden Mainstream Viren keine 0day Exploits, um die Systeme zu kompromittieren. Die relativ teuren Angriffe mit 0day Exploits werden nur für gezielte Angriff auf besondere Ziele eingesetzt, und nicht bei Viren. Computer Viren nutzen in Regel längst bekannte Lücken in der Software aus, die in verschiedenen Quellen nach der Beseitigung durch den Softwarehrsteller publiziert wurden.

   Regelmäßige Updates der verwendeten Software und sichere Konfiguration des Systems schützen besser gegen die Angriffe mit Viren, als ein Virenscanner.

   Hinweis: zur sicheren Konfiguration gehört als erstes, dass man die Einstellungen der Benutzerkontensteuerung auf die höchste Sicherheitsstufe stellt. Es ist bedauerlich, dass Microsoft dieses Sicherheitsfeature nicht standardmäßig aktiviert.

5. Gegen potente Angreifer, die ein Target gezielt mit staatlich subventionierten Trojanern angreifen, können (und wollen?) kommerzielle Virescanner nicht schützen. Das konnte man anhand der Veröffentlichungen zur NSA-Cyberwaffe *Regin* verfolgen.

   - Als erstes hat Fox-IT den Trojaner *Regin* bei der Analyse des Einbruchs bei Belacom gefunden. Es wurde aber nichts veröffentlicht und die Signaturen wurden nicht in die Datenbank für Kunden

[10] https://heise.de/-2482344
[11] https://heise.de/-3095024
[12] https://heise.de/-3620159

aufgenommen. Ronald Prins von Fix-IT sagte nach der Veröffentlichung von *Regin* durch The Intercept im Nov. 2014:

> *We didn't want to interfere with NSA/GCHQ operations. Everyone seemed to be waiting for someone else to disclose details of Regin first, not wanting to impede legitimate operations related to global security.*

- Dann wurde der Trojaner *Regin* von Symantec analysiert. Auch Symantec veröffentlichte nichts. Vikram Thakur von Symantec sagte im Nov. 2014 als Entschuldigung:

  > *We had been investigating Regin since last year, but only felt comfortable publishing details of it now.*

- Im Sommer 2014 wurde *Regin* auf dem Laptop einer Mitarbeiterin im Bundeskanzleramt gefunden. Auch über diesen Vorfall wurde geschwiegen, bis die Bild Zeitung im Dez. 2014 (nach der Veröffentlichung von The Intercept) den Vorgang marktschreierisch veröffentlichte. Die Bundesregierung wollte diese NSA-Spionage anfangs nicht kommentieren und dementierte halbherzig.
- Erst nachdem The Intercept im Nov. 2014 ankündigte, über *Regin* zu berichten, haben die Anti-Virus Firmen reagiert und sind ebenfalls an die Öffentlichkeit gegangen.

MacOS

Wenn man die Apple Datenschutzrichtlinie liest, erkennt man, das MacOS sich nicht als Betriebssystem eignet, wenn man seine Privatsphäre nicht mit Apple teilen möchte:

> *Wir erheben Daten wie namentlich Beruf, Sprache, Postleitzahl, Vorwahl, individuelle Geräteidentifizierungsmerkmale, Weiterleitungs-URL sowie Ort und Zeitzone, wo Apple Produkte verwendet werden, damit wir das Verhalten unserer Kunden besser verstehen und unsere Produkte, Dienste und Werbung verbessern können.*

Für diese Datensammlungen wurde Apple mit dem BigBrother Award 2011 geehrt. Apple ist seit Oktober 2012 Partner im PRISM Programm der NSA.

Linux

Es gibt eine Vielzahl von Linux Distributionen, so dass man als potentieller Anwender erst einmal vor der Qual der Wahl steht: Debian und Derivate, OpenSuSE, OpenMandriva, Fedora, Gentoo für Bastler, Minidistributionen wie Puppy oder Fortress Linux als besonders gehärtete Variante, KaliLinux... Ich kenne längst nicht alle Distributionen daher nur einige Gedanken:

- **Debian** ist ein robustes Arbeitstier unter den Linux Distributionen. Die Maintainer legen vor allem Wert auf Stabilität und weniger auf neueste Features. In Kombination mit den langen Release Zyklen ergibt sich ein System, das mit brandneuer Software und Hardware (insbesondere Laptops) öfters Probleme hat, aber nach erfolgreicher Installation lange Zeit stabil läuft. Debian hatte als erste Distribution Full-Disc-Encryption bei der Installation angeboten.

- **Ubuntu** ist angetreten, um das bessere Debian zu sein und mit aktueller Software auch neueste Hardware gut zu unterstützen. In letzter Zeit geht das Projekt oft eigene Wege und die Übertragung sämtlicher Suchanfragen bei Nutzung des Unity Desktop an kommerzielle Dritte wie z.B. Amazon ist ein Fiasko für die Privatsphäre. Man kann diese Probleme aber beseitigen, siehe FixUbuntu.com.[13]

  1. Das Unity Tweak Tool installieren und starten. Auf der Kommandozeile:

     ```
     > sudo apt install unity-tweak-tool
     > unity-tweak-tool
     ```

  2. Auf dem Reiter *Suche* ist das *Durchsuchen von Online Quellen* sowie *Mehr Empfehlungen anzeigen* zu deaktivieren.

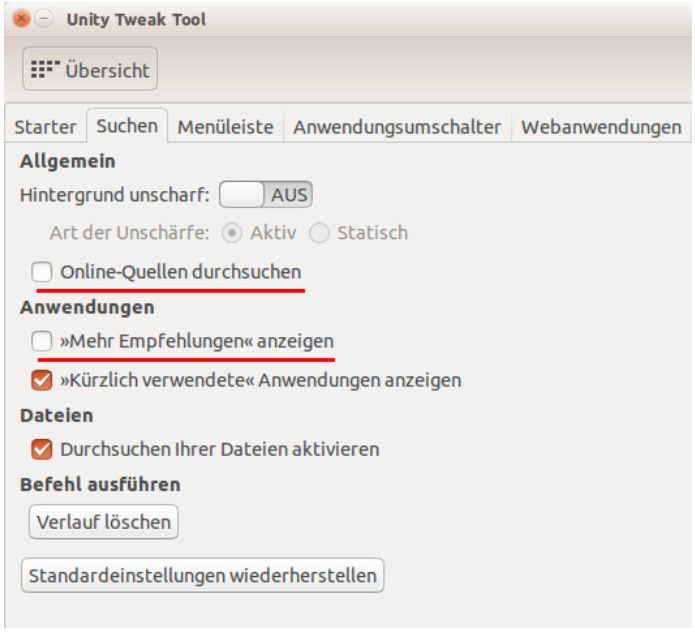


Abbildung 17.1: Privacy Einstellungen im Unity Tweak Tool

Hinweis: die Datenübertragung betrifft nur das orginale Ubuntu mit dem Unity Desktop. Derivate mit anderen Desktops wie Xubuntu (verwendet XFCE statt Unity) oder Kubuntu (KDE statt Unity) benötigen keine Anpassungen mit dem Tweak Tool.

Daneben gibt es weitere privacy-invasive Tools in Ubuntu, die ständig irgendwelche Ubuntu-Server kontaktieren. Einige kann man problemlos deinstallieren wie den Crash Reporter *apport* und das Report Submission

[13] https://fixubuntu.com/

Tool *whoopsie*, das täglich den Server daisy.ubuntu.com kontaktiert. Andere Tools sind aber eng mit dem Unity Desktop verflochten, wie das Location Tracking Tool *geoclue*, das den Unity Anwendungen Informationen über die aktuelle Position zur Verfügung stellt, oder das Logging Tool *Zeitgeist*, welches alle Aktivitäten protokolliert. Um diese Tools zu deinstallieren, müsste man zuerst einen anderen Desktop installieren. Dann kann man aber auch gleich Xubuntu oder Kubuntu wählen.

- **Ubuntu LTS** (Long Term Support): neben der halbjährlich aktualisierten Distribution gibt es Ubuntu in einer LTS Version, die man nur alle zwei Jahre komplett aktualisieren muss. Ich rate davon ab, diese Version auf dem Desktop zu nutzen. Der Long Term Support gilt nur für die 9.000 Pakete des Main-Repository. Der Rest der 45.000 wird nur mangelhaft mit Sicherheitsupdates versorgt.

- **Xubuntu** oder **Kubuntu** gefallen mi ram besten. Die gute Hardware Unterstützung für neue Technik kombiniert mit einfacher Installation, klarem Bedienkonzept des Desktop ohne irgendwelche Cloud Anbindungen oder Übertragung von Daten an Dritte sowie Full-Disc-Encryption bei der Installation mag ich.

  Den privacy-invasiven Crash Reporter von Ubuntu und das Report Submission Tool *whoopsie*, das täglich den Server daisy.ubuntu.com kontaktiert, kann man nach der Installation problemlos mit der bevorzugten Paketverwaltung entfernen. Im Terminal erledigt man das mit:

  ```
  > sudo apt purge whoopsie apport
  ```

  Die Deinstallation überflüssiger Software ist ein Sicherheitsfeature. Ein Bug im Crash Reporter *apport* konnte beispielsweise jahrelang dazu genutzt werden, um den Rechner aus der Ferne zu kompromittieren.[14]

- **Mint Linux** möchte das bessere Ubuntu sein und bietet vor allem einen anderen Desktop, der auch sehr hübsch ist. Allerdings ist Mint keine komplett selbständige Distribution sondern schmarotzt bei Ubuntu, was öfters für Verstimmung bei Canonical sorgte und die Probleme mit der mangelhaften Versorgung für Sicherheitsupdates einschließt. Mit Mint Debian Edition gibt es auch eine Variante, die auf Debian basiert.

- **elementary OS** möchte das hübschere Ubuntu sein. Diese Distribution basiert auf Ubuntu LTS und möchte einen besonders schönen und konsistenten Desktop bieten, der sich sehr an MacOS orientiert. Um ein einheitliches Bild der Anwendungen zu bieten sind Cross-Plattform Programme wie Firefox, Thunderbird oder LibreOffice in der Standardinstallation nicht enthalten. Es werden nur native GTK+ Anwendungen installiert, aber Firefox und Thunderbird können aus den Repositories nachträglich installiert werden.

[14] http://www.golem.de/news/linux-sicherheit-ubuntu-bug-ermoeglicht-das-ausfuehren-von-schadcode-1612-125112.html

- **Qubes OS** ist eine Besonderheit unter den Linux Distributionen. Alle Anwendungen laufen in mehreren getrennten virtuellen Maschinen mit einem Xen-basierten Hypervisor, der die Gastsysteme überwacht und ihnen nur begrenzt Zugriff auf die Hardware lässt. Qubes OS bietet:
  - Schutz durch starke Isolation der einzelnen Anwendungen
  - getrennter Netzwerkzugriff für jede der VMs
  - umfangreiche graphische Integration der virtuellen Maschinen inklusive Farben zur visuellen Abgrenzung der VMs untereinander

  Nachteilig ist der wesentlich höhere Speicherbedarf als alle anderen bekannten Betriebssysteme/Distributionen.

- **Subgraph OS**[15] ist ein Linux basiertes Betriebssystem, das hinsichtlich Sicherheit und für anonyme Kommunikation optimiert wurde. Es kann als Live-DVD als Alternative TAILS genutzt werden oder ist als Linux Distribution auf der Festplatte installierbar. Derzeit steht erst eine Alpha-Version zum Download bereit, die noch nicht für den produktiven Einsatz freigegeben wurde. Features von Subgraph OS sind:
  - Out-of-the-box-ready für anonyme, sichere und trackingfreie Kommunikation.
  - Es wird ein besonders gehärteter Linux Kernel genutzt (Grsecurity/PaX).
  - Einzelnen Anwendungen sind in Sandboxen gegeneinander abgeschirmt.
  - Der gesamte Datenverkehr wird über Tor Onion Router anonymisiert. Als Standardbrowser wird der TorBrowser eingesetzt. Dabei wird im Gegensatz zu TAILS sichergestellt, dass verschiedene Anwendungen unterschiedliche Routen durch das Tor Netz nutzen, so dass der Traffic 100% separiert ist.
  - Nur eine limitierte Anzahl von Anwendungen hat Zugriff auf das Internet via Tor.
  - Installation von Subgraph OS ist nur mit verschlüsseltem Dateisystem möglich.

Bei allen Linux Distributionen erhält man nach einem einfachen Installationsprozess, der auch für Laien durchführbar ist, ein lauffähiges System mit wesentlich umfangreicherer Software, als mit Windows oder MacOS. Gleichzeitig ist das System umfangreich anpassbar und unter Kontrolle des Anwenders, der *root* sein kann. Die bekannten Programme wird ein Umsteiger von Windows vergeblich suchen, es gibt kein Photoshop, keinen Windows Explorer oder MS Office, dafür gibt es zahlreiche Alternativen.

NetBSD und OpenBSD

Diese beiden BSDs sind konsequent und ohne Kompromisse hinsichtlich Benutzbarkeit auf Sicherheit optimiert. Wenn man mehrere Jahre Erfahrung mit

[15] https://subgraph.com/sgos/index.en.html

mit einem UNIX-artigen System (z.B. Linux) gesammelt hat und hinreichend leidensfähig ist, dann kann man auch diese beiden Betriebssstem einsetzen und sich an den Vorteilen erfreuen.

Die Optimierung auf Sicherheit gilt nur für das Betriebssystem, nicht für Anwendungen oder zusätzliche Bibliotheken. Gelegentlich werden Sicherheitsfeatures von Bibliotheken wie z.B. OpenSSL unterlaufen, denen das sichere Allocieren von Speicher bei NetBSD und OpenBSD zu langsam war und deren eigene Implementierung dann zum Heartbleed Bug führte.

Anwendungen wie X11, Mozilla Firefox oder Thunderbird lassen sich in der höchsten Sicherheitsstufe von NetBSD und OpenBSD nicht installieren. In NetBSD muss man in der Datei /etc/mk.conf folgende Option setzen:

```
ALLOW_VULNERABLE_PACKAGES=yes
```

17.1 Risiko USB, Firewire und Thunderbolt

Die Nutzung der **USB** Schnittstellen ist weit verbreitet und bedenkenlos werden Speichermedien (USB-Sticks oder USB-Festplatten), Kameras, Smartphones, Drucker und andere Peripheriegeräte an den Computer oder Laptop angeschlossen. Zunehmend wird die USB-Schnittstelle auch zum Aufladen von Geräten genutzt, die eigentlich keine Funktion in Zusammenhang mit dem Computer erfüllen.

Sogenannte BadUSB Devices müssen kaum Sicherheitshürden überwinden und auch keine 0-day Exploits einsetzen. Sie können die vielfältigen technischen Features neu kombinieren, um unschöne Dinge anzustellen. USB-Geräte (z.B. USB-Sticks von Fremden) können neben der sichtbaren Funktion (z.B. als Speichermedium) weitere verdeckte Funktionen enthalten, die man nicht bemerkt. Sie können sich heimlich als USB-Tastatur ausgeben und Kommandos senden oder sich als Netzwerkkarten ausgeben und Datenverkehr umleiten.

- Auf der Blackhat 2014 haben K. Nohl und J. Lell von SRLabs im Vortrag *BadUSB - On Accessories that Turn Evil*[16] gezeigt, wie der Internettraffic für bestimmte Webseiten umgeleitet wird, ohne das der User etwas merkt. Wenn man es einmal ausprobieren möchte, kann man sich das Script BadAndroid-v0.1.zip von SRLabs herunter laden. Das Archiv enthält eine README und ein Script, welches man auf ein gerootetes Android Smartphone kopiert und dort startet. Dann schließt man das Smartphone an einen Computer an (Windows oder Linux) und ... - eine nette Demo.

- Im Nov. 2016 hat Samy Kamkar mit PoisonTap[17] ein weiteres BadUSB Device vorgestellt. Wenn der Angreifer physischen Zugang zu einem Computer oder Laptop mit aktiviertem Passwortschutz hat (z.B. durch Bildschirmschoner) und auf dem Rechner noch ein Browser geöffnet ist,

[16] https://www.youtube.com/watch?v=nuruzFqMgIw
[17] https://www.schneier.com/blog/archives/2016/11/hacking_passwor.html

dann kann PoisonTab mit einigen kleinen Tricks die Online Accounts (E-Mail, Twitter, Facebook...) des Targets übernehmen, die mit diesem Browser genutzt wurden. Der Angreifer muss nur *PoisonTab* am USB Port anschließen und warten.

Ein besonderes Risiko sind USB-Sticks oder USB-Festplatten, die man bedenkenlos an unterschiedlichen Computern in verschiedenen Netzen nutzt.

- Ein Beispiel aus der Praxis: Vor einigen Jahren war ich für ein paar Monate als IT-Administrator für eine Firma tätig. Dort habe ich einmal eine Woche lang jeden Tag den gleichen Virus gejagt. Am Abend war das Firmennetzwerk sauber, am nächsten Morgen war der Virus wieder da. Eine Sekretärin hatte am Abend Dokumente mit nach Hause genommen und am Morgen mit dem verseuchten USB-Stick den Virus von ihrem schlampig gewarteten Computer zuhause wieder ins Firmennetzwerk eingeschleppt.
- Einige spektakuläre Beispiele aus den Medien zeigen, dass es im Cyberwar üblich ist, Malware auf USB-Stick in schwer zugängliche Netzen zu transportieren. Dabei kann der USB-Stick extra präpariert werden oder man greift die schlecht gesicherten Rechner mehrere Targets zuhause an und hofft, dass der Trojaner von einem Wirt mit einem USB-Stick in das gesicherte Netzwerk getragen wird.
  - 2008 wurde ein niedlicher USB-Stick auf einer US-Militärbasis in Nahost platziert. Eine Knallcharge steckte den Stick in seinen Computer und infizierte das gesamte Kommunikationssystem des US-Militärs (klassifizierte und nichtklassifizierte Netzwerke) mit dem russischen Trojaner *agent.bz*. Es dauerte 14 Monate und kostete mehrere Mio. Dollar, die Netzwerke zu säubern.
  - *Stuxnet* wurde von einem Mossad Agenten mit einem USB-Stick in die Uranaufbereitungsanlage im Iran gebracht.
  - *Regin* ist ein hochentwickelter Spionage-Trojaner der NSA. . Dieser Trojaner konnte 2014 ins Bundeskanzleramt gelangen und dann dort seine Aufgaben ausführen, weil eine Mitarbeiterin dienstliche Dokumente zuhause auf dem infizierten PC bearbeitete und mit dem USB-Stick ins Bundeskanzleramt brachte.

Bei **Firewire** (IEEE 1394) und **Thunderbolt** Schnittstellen ist das Risiko noch größer. Im Gegensatz zu USB wird bei diesen Schnittstellen keine Master-Slave Kommunikation genutzt. Über Firewire und Thunderbolt haben angeschlossene Geräte via DMA (Direct Memory Access) vollen Zugriff auf den Hauptspeicher des PC und können z.B. eine Kopie auslesen.

- 2008 wurde demonstriert, wie man den Windows Login mit einem Firewire Gerät umgehen kann. Microsoft sah keinen Handlungsbedarf, da die Funktionalität der Firewire Spezifikation entspricht. Es ist also kein Bug sondern ein Feature.
- Gegen Aples I/O-Technik Thunderbolt gab es von Anfang an Sicherheitsbedenken[18]. Dokumente von HBGary belegen, dass US-Behörden schon

[18] http://heise.de/-1198049

2011 ein Framework nutzen, um Trojaner via Thunderbolt auf PCs und Laptops zu installieren.

- Die Datenverschlüsselung kann umgangen werden (für alle Produkte), da Keys aus dem Hauptspeicher ausgelesen werden können. Geheimdienste nutzen passende Tools routiniert, wenn sie physischen Zugriff auf den Zielrechner haben.

Hinweise zur Verbesserung der Sicherheit

1. Ein USB-Stick, der an einen unbekannten Computer angeschlossen wurde, oder ein USB-Stick von Dritten ist als potentiell verseucht zu betrachten. Man kann das Risiko verringern, wenn man eine Live-DVD nutzt.

2. Um Daten von USB-Sticks zu bearbeiten oder Fotos von der Digicam auf einer USB-Festplatte zu archivieren, kann man eine Live-DVD nutzen. Insbesondere sollte man eine Live-DVD nutzen, wenn man Daten aus der Firma zuhause bearbeiten und wieder mit in die Firma nehmen will.

3. Zum Aufladen von Geräten kann man USB-Ladegeräte nutzen. Man muss nicht alles, was wie ein USB-Stecker aussieht, in den Computer einführen. Das BSI warnt sogar davor, E-Zigaretten via USB-Anschluss am Computer aufzuladen und rät zu einem USB-Ladegerät.[19]

4. *USBGuard* für Linux[20] zeigt dem Nutzer an, welcher Gerätetyp angeschlossen wird. Man kann dann das Gerät zulassen oder blockieren, noch bevor das zugehörige Modul des Linux-Kernels das Gerät anspricht und eine Verbindung aufbaut. Auch dauerhaftes Zulassen/Blockieren nach Geräteklasse oder ID kann konfiguriert werden.

5. Es gibt zahlreiche Freeware Tools, um USB-Schnittstellen unter Windows zu sperren. (z.B. den USB-Blocker[21] von securityXploded.com)

6. Wenn man Firewire nicht nutzt, sollte man alle Firewire Schnittstellen deaktivieren.

   - Für Windows stellt MS einen Support Artikel bereit: *Blockieren des SBP-2-Treibers und der Thunderbolt-Controller, um Bedrohungen für BitLocker zu reduzieren*.[22]
   - Unter Linux kann man prüfen, ob das System Firewire Schnittstellen beim Booten erkannt hat:

     ```
     > lspci | grep -i Firewire
     ```

     Wenn der Rechner Firewire Schnittstellen hat, dann kann man die Kernelmodule für diese Schnittstellen sperren. Man speichert eine Datei *firewire.conf* im Verzeichnis */etc/modprobe.d/* mit folgendem Inhalt:

[19] http://heise.de/-3222811
[20] https://dkopecek.github.io/usbguard/
[21] http://securityxploded.com/windows-usb-blocker.php
[22] https://support.microsoft.com/kb/2516445/de

```
blacklist firewire-ohci
blacklist firewire-sbp2
```

Danach führt man folgende Kommandos aus:

```
> sudo depmod -ae
> sudo update-initramfs -u
```

17.2 Linux Firewall konfigurieren

Die Firewall des Linux Kernels wird mit dem Tool *iptables* konfiguriert. Es gibt einige GUIs für die Konfiguration, die irgendwelche Regeln zusammenstellen und eine Firewall verwalten können. Volle Kontrolle über die Firewall hat man aber nur, wenn man es selbst macht. Eine Firewall mit *iptables* selbst zu konfigurieren, ist nicht so schwer. Einfache Dinge sind einfach und Kompliziertes ist möglich.

Man kann für alle Distributionen Shell-Script mit der Firewall Konfiguration im Verzeichnis */etc/network/if-up.d* speichern. Das Script wird dann nach dem Herstellen einer Netzwerkverbindung ausgeführt und aktiviert die Firewall Regeln. Eine einfache Firewall Basis-Konfiguration für Desktop Rechner oder Laptops blockiert alle Verbindungsversuche von außen und erlaubt es allen Nutzern und Daemonen, Verbindungen ins Internet herzustellen:

```
#!/bin/sh
set -e

# Nichts tun, wenn loopback aktiviert wird
[ "$IFACE" != "lo" ] || exit 0

# alte Konfiguration löschen
/sbin/iptables --flush
/sbin/iptables --delete-chain
/sbin/iptables -t mangle --flush
/sbin/iptables -t mangle --delete-chain
/sbin/iptables -t nat --flush
/sbin/iptables -t nat --delete-chain

# forwarding deaktivieren
echo 0 > /proc/sys/net/ipv4/ip_forward

# Default-Policies setzen
/sbin/iptables -P INPUT DROP
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT

# loopback freischalten
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -i lo -j ACCEPT
```

```
# Antworten auf bestehende Verbindungen erlauben
/sbin/iptables -A INPUT -i $IFACE -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Das Script kann man von meiner Webseite herunter laden. Nach dem Download ist das Script in das Verzeichnis */etc/network/if-up.d* zu kopieren (1) und als *ausführbar* zu markieren (2). Für beide Schritte sind root Rechte erforderlich.

```
(1) > sudo cp Downloads/090firewall /etc/network/if-up.d
(2) > sudo chmod +x /etc/network/if-up.d/090firewall
```

Diese Firewall Konfiguration ist stealth. Der Rechner beantwortet keine Pings und ist nicht mit Portscans im lokalen Netz auffindbar.

Erweiterungen der Basiskonfiguration - Teil 1

Wenn Dienste auf dem Rechner von außen erreichbar sein sollen, dann kann man weitere Regeln anfügen, um einzeln Ports zu öffnen. Als Beispiel soll der Port 8888 (für den I2P-Router) für eingehenden TCP und UDP Traffic geöffnet werden:

```
/sbin/iptables -A INPUT -i $IFACE -p tcp --dport 8888 -j ACCEPT
/sbin/iptables -A INPUT -i $IFACE -p udp --dport 8888 -j ACCEPT
```

Erweiterungen der Basiskonfiguration - Teil 2

Wenn nur bestimmte User und Daemonen Verbindungen ins Internet herstellen dürfen, kann man zusätzliche OUTPUT Regeln einfügen, die diesen UIDs den Aufbau von Verbindungen ins Internet ausdrücklich erlaubt und dann alle anderen Verbindungsversuche abweisen. Zuerst muss man das Kernelmodul *ipt_owner* laden:

```
modprobe ipt_owner
```

Die Regeln werden nach folgendem Muster definiert:

```
# Freigabe definieren
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner <user> -j ACCEPT

# den Rest blockieren
/sbin/iptables -t filter -A OUTPUT -j REJECT
```

Dafür sollte man sein System aber gut kennen und wissen, welche Dienste man benötigt. Ein kleines Beispiel als Anregung für eigene Experimente:

- Es soll nur dem Nutzer *inetuser* gestattet werden, im Internet zu surfen und Tor bzw. JonDo zu verwenden. Dafür reicht es, die Ports 80 und 443 für ausgehende TCP Verbindungen zu öffnen.
- Der DNScrypt-proxy kümmert sich um die Auflösung der DNS-Namen beim Surfen ohne Tor oder JonDo und läuft unter der UID *dnscrypt*.
- Alle weiteren Tools zur Kommunikation werden mit Tor oder JonDo (Premium) anonymisiert, beide Anon-Dienste können Port 443 verwenden.

Dafür sind folgende Regeln nötig:

```
# Freigaben
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner inetuser \
               -p tcp --dport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner inetuser \
               -p tcp --dport 443 -j ACCEPT
/sbin/iptables -A OUTPUT -o $IFACE -m owner --uid-owner dnscrypt \
               -p udp --dport 443 -j ACCEPT

# den Rest blockieren
/sbin/iptables -t filter -A OUTPUT -j REJECT
```

Was passiert, wenn man als *root* die Software aktualisieren will oder Software aus den Repositories installieren will? *root* kann keine Verbindungen ins Internet aufbauen. Entweder man nutzt Tor bzw. JonDo dafür, oder man fügt temporär eine weitere Regel für *root* hinzu. Viele Spielchen sind möglich.

Erweiterungen der Basiskonfiguration - Teil 3

Mit der Option -d (–destination) kann man zulässige IP-Adressen oder Netzwerkbereiche für ausgehenden Traffic definieren. Man könnte im Beispiel oben z.B. eine OUTPUT Regel vor der letzten REJECT Regel einfügen, die Verbindungen zu einem CUPS Netzwerkdrucker erlaubt. Die IP-Adresse des Netzwerkdrucker ist in diesem Beispiel 192.168.1.30.

```
# Verbindungen zum Netzwerkdrucker erlauben
/sbin/iptables -A OUTPUT -o $IFACE -p tcp -d 192.168.1.30 \
               --dport 631 -j ACCEPT
```

In Firmen könnte man pauschal Verbindungen zu allen Netzwerkdruckern im lokalen Netz erlauben, indem man den gesamten Netzwerkbereich 192.168.1.* freigibt:

```
# Verbindungen zu allen Netzwerkdruckern im LAN erlauben
/sbin/iptables -A OUTPUT -o $IFACE -p tcp -d 192.168.1.0/24 \
               --dport 631 -j ACCEPT
```

Prinzipiell kann man auch Hostnamen statt IP-Adressen verwenden. Die DNS-Auflösung der Hostnamen erfolgt aber nur einmalig vor der Übergabe der Regeln an den Kernel.

Logging

Zur Erkennung von Angriffsversuchen oder um Probleme mit eigenen, restriktiven Konfigurationen zu erkennen, kann man Logging in *iptables* aktivieren.

```
# Logging aktivieren
/sbin/iptables -N LOGGING
/sbin/iptables -A INPUT -j LOGGING
/sbin/iptables -A OUTPUT -j LOGGING
/sbin/iptables -A LOGGING -m limit --limit 2/min -j LOG \
               --log-prefix "IPTables-Dropped: " --log-level 4
/sbin/iptables -A LOGGING -j DROP
```

Dieses Beispiel schreibt die Logs über gedroppte Paket nach */var/log/syslog*. Die Zeilen beginnen mit *IPTables-Dropped:*, so dass man mit schnell filtern kann.

17.3 WLAN Privacy Leaks

Wenn man mit dem Laptop unterwegs ist und WLANs in Internet Cafe's, am Flughafen, in der Firma oder im Hotel nutzt, dann bekommt man die Netzwerkkonfiguration (eigene IP-Adresse, DNS-Server...) via DHCP-Protokoll zugeteilt. Damit hinterlässt man auf dem DHCP-Server Spuren, die C. Huitema von der IETF in der Studie *Unique Identifiers in DHCP options enable device tracking*[23] zusammengefasst hat:

1. Die MAC-Adresse wird an den DHCP-Server übermittelt und ist eine weltweit eindeutige Kennung für die Hardware des Rechners (Netzwerkschnittstelle oder WLAN-Modul).

   - In IPv4 Netzen wird diese Kennung nur bis zum Router/Gateway übertragen. Im eigenen Home-Netz braucht man sich also keine Gedanken machen, aber in fremden WLANs (Hotel, Internetcafe', Flughafen) ist davon auszugehen, dass die MAC-Adressen der Nutzer protokolliert werden.
   - In IPv6 Netzen wird die MAC-Adresse Bestandteil der IP-Adresse, wenn die *Privacy Extension for IPv6* nicht aktiviert wurde. Damit wird die IP-Adresse zu einem personenbezogenen Merkmal und kann zur Wiedererkennung und zum Tracking genutzt werden.

2. Die UUID/GUID des Intel Preboot eXecution Environment (PXE) wird an den DHCP-Server übermittelt, wenn PXE in den BIOS Einstellungen aktiv ist. PXE kann im BIOS deaktiviert werden.

3. Der konfigurierte Hostname und die DNS-Domain des Rechners wird an den DHCP-Server übermittelt.

Wenn man die automatische Anmeldung für die bevorzugte WLANs aktiviert hat, dann sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte *Probes*, um die Umgebung nach den bevorzugten WLANs zu scannen.

- Die *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Studie *Why MAC Address Randomization is not Enough* demonstrierte.[24]

- Mit den *Probes* auch eine Liste der bevorzugten WLANs gesendet, mit denen sich der Laptop automatisch verbinden würde (Prefered Network List, PNL). Diese Prefered Network List liefert Informationen über Orte, an denen sich der Besitzer des Laptops bevorzugt aufhält.

[23] https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00
[24] https://tools.ietf.org/html/draft-huitema-perpass-dhcp-identifiers-00

- Praktische Angriffe mit den Informationen aus den *Probes* hat die Security Firma Sensepost mit der Drohne *Snoopy* vorgestellt. Diese Drohne simuliert die SSID eines bevorzugten WLANs. Der Laptop meldet sich automatisch bei der Drohne an, der Internet Traffic läuft über die Drohne und kann dort analysiert werden. Es wurde z.B. demonstriert, wie Snoopy die Login Credentials für PayPal, Yahoo! usw. abreifen konnte.[25]

Um keine eindeutigen Spuren als Road-Warrior in Internet Cafe's oder am Flughafen zu hinterlassen, kann man die MAC-Adresse faken, automatische Anmeldung für alle WLANs deaktivieren, PXE Boot im BIOS des Rechners deaktivieren und nichtssagenden Hostnamen und DNS-Domain nutzen.

17.3.1 MAC-Adresse faken für Linux

Der *NetworkManager v. 1.2* arbeitet ein bisschen privacy-freundlich. Beim Suchen nach WLANs wird eine gefakte MAC-Adresse verwendet und man kann diesen Fake auch für die Verbindung nutzen. Für IPv6 werden die Privacy Extensions sowie die in RFC 7217 festgelegten Methoden genutzt, um eine Wiedererkennung zu verhindern. Die Version 1.2 des NetworkManager in aktuellen Distributionen wie Ubuntu 16.04+ und Derivaten bereits enthalten.

Die Analyse *Why MAC Address Randomization is not Enough* des CITI zeigte, dass mit Hotspot 2.0 Honeypots trotzdem die reale MAC Adresse ermittelt werden kann. Die Installation von *macchanger* ist also trotzdem notwendig, um auch gegen ernsthafte Trackingversuche geschützt zu sein.

Das Tool **macchanger** gibt es für alle Linux Distributionen, man kann es mit dem bevorzugten Paketmanager installieren. Unter Debian oder Ubuntu kann man apt-get nutzen:

```
> sudo apt-get install macchanger
```

Bei der Installation kann man festlegen, dass bei jedem Aufbau einer Netzwerkverbindung (Kabel oder WLAN) automatisch ein neuer Fake genutzt werden soll - Fertig. Wenn man die Auswahl später (temporär) ändern möchte, kann man das Kommando zur Re-Konfiguration des Paketes nutzen:

```
> sudo dpkg-reconfigure macchanger
```

Wenn man die *automatische Anmeldung* für bevorzugte WLANs aktiviert hat, dann sendet der Laptop unterwegs (am Flughafen, im Hotel, in der U-Bahn...) ständig sogenannte *Probes*, um die Umgebung nach den bevorzugten WLANs zu scannen. Diese *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden, wie die Analyse *Why MAC Address Randomization is not Enough* demonstrierte.

In den Einstellungen der WLAN-Verbindungen muss man für alle konfigurierten WLANs die Option zum automatischen Verbinden abschalten,

[25] http://www.golem.de/news/drohne-snoopy-schnueffelt-im-vorbeiflug-1403-105329.html

um *Probes* zu vermeiden. Die Option findet man auf dem Reiter *Allgemeine Einstellungen* der jeweiligen Netzwerkverbindung im Verbindungs-Editor.

Wenn man *macchanger* aktiviert hat, dann wird für jeden Verbindungsaufbau ein neuer Fake für die MAC-Adresse verwendet. Unter Umständen ist dieses Verhalten unerwünscht und man möchte immer den gleichen Fake verwenden (z.B. wenn man sein WLAN zuhause sicher konfiguriert hat und nur bestimmten MAC Adressen den Zugang erlauben möchte, wenn der Zugang in der Firma nur für bestimmten MAC-Adressen möglich ist oder wenn man im Hotel den Wi-Fi Zugang für mehrere Tage bezahlt hat).

In den Einstellungen für Netzwerkverbindungen kann man unter dem Reiter *Wi-Fi* für einzelne WLAN Netzwerke feste Fakes für die MAC-Adressse konfigurieren. Eine zufällige MAC-Adresse für diesen Zweck kann man einfach mit Klick auf den Button *Zufällig ...* generieren lassen.

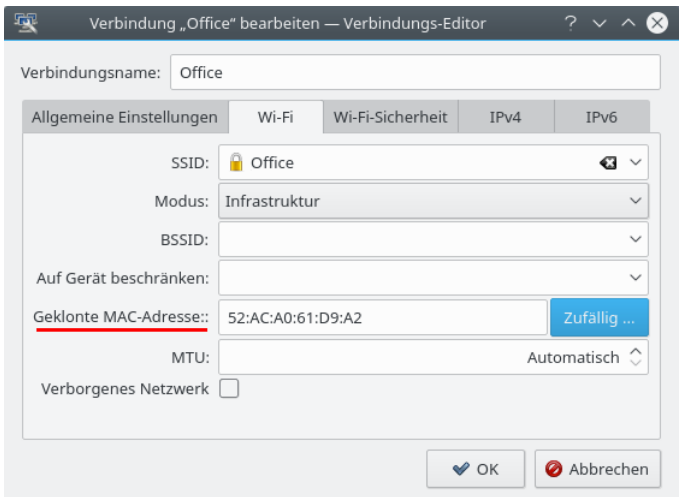


Abbildung 17.2: Fixed Fake für MAC-Adresse konfigurieren

Idealerweise Weise konfiguriert man diese Einstellungen, bevor man sich das erste Mal mit einem Wi-Fi Netzwerk verbindet (z.B. im Hotel).

17.3.2 MAC-Adresse faken für Windows 10

Windows 10 enthält alles, was man braucht, um die MAC-Adressen für WLAN-Verbindungen zu faken. Bevor(!) man sich unterwegs im Hotel, am Flughafen oder in der Berliner U-Bahn mit einem neuen WLAN verbindet, kann man die Randomisierung der MAC-Adresse aktivieren. Die Einstellungen werden alle in der Sektion *Netzwerk und Internet* auf dem Reiter *Wi-Fi* vorgenommen, siehe Bild 17.3.

1. Als erstes muss man unter *Manage Wi-Fi settings* die Randomisierung der MAC Adressen global einschalten, damit diese Funktion danach für ein-

zelne WLANs konfiguriert werden kann. Außerdem wird immer eine zufällige MAC-Adresse für den Scan nach WLANs verwendet, wenn die Randomisierung global aktiviert wurde.

2. Danach muss man das WLAN-Netzwerk wählen und unter *Advanced Options* für jedes Netzwerk einzeln den Modus für den Fake der MAC-Adresse auswählen. Man kann täglich eine neue MAC-Adresse generieren lassen oder den gleichen Fake immer wieder nutzen. Das ist z.B. für Wi-Fi Hotspots in Hotels sinnvoll, bei denen man für mehrere Tage bezahlt hat, oder wenn der Zugang zu einem Firmen-WLAN anhand der MAC-Adressen limitiert wird.

3. Die Option *automatisch Verbinden* sollte man für alle WLANs deaktivieren. Wenn die Option für ein oder mehrere WLAN Verbindungen aktiviert wurde, dann sendet der Rechner ständig sogenannte *Probes*, um aktiv nach diesen WLANs in der Umgebung zu suchen. Die *Probes* haben einen eindeutigen Fingerprint und können in gleicher Weise wie MAC-Adressen für das Tracking der Geräte verwendet werden.

4. Dann kann man sich mit dem WLAN verbinden.

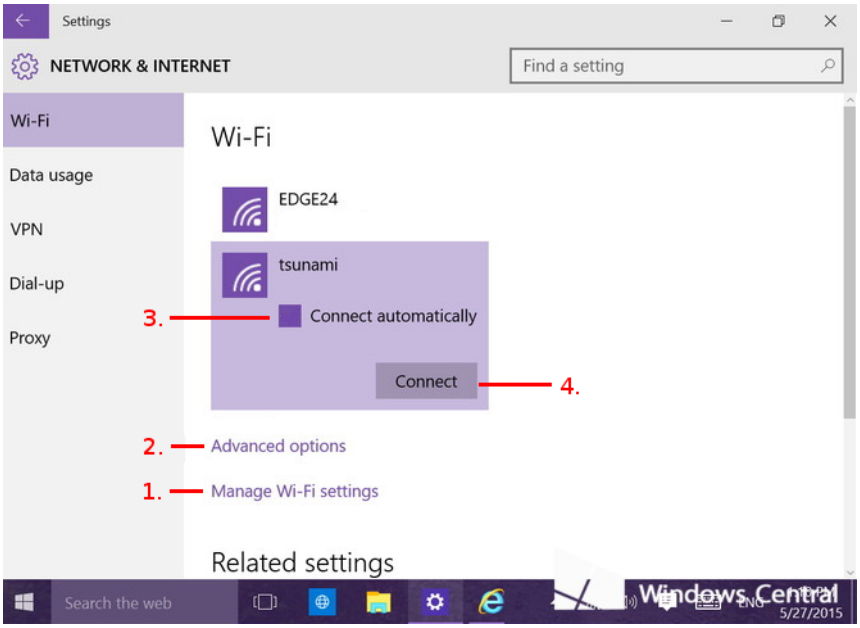


Abbildung 17.3: MAC-Adresse faken für Windows 10

17.3.3 Hostname und DNS-Domain konfigurieren

Hostname und Domain kann man bei der Installation des Betriebssystems festlegen oder nachträglich ändern. Es gibt keine wirklich anonyme Empfehlung für diese Werte. Wir empfehlen die folgende nichts aussagende Werte, die auch von Live-DVDs wie TAILS u.a. verwendet werden:

```
Hostname: host
Domain:   localdomain
```

Wenn man Linux verwendet, kann man den Hostnamen nachträglich mit folgenden Kommandos ändern:

```
> sudo hostname host
```

Um die DNS-Domain unter Linux nachträglich zu ändern, sind folgende Zeilen in der Datei */etc/hosts* anzupassen:

```
127.0.0.1 host.localdomain host
::1 host.localdomain host
```

Man kann den NetworkManager auch dazu überreden, beim Aufbau einer Netzwerkverbindung keinen den Hostnamen an den DHCP-Server zu senden. Dafür sind folgende Zeilen in der Datei */etc/NetworkManager/NetworkManager.conf* einzutragen:

```
[ipv4]
dhcp-send-hostname=false
```

Kapitel 18

Live-DVDs

Es gibt einige Projekte, die fertig konfigurierte Live-DVDs bereitstellen. Bei der Nutzung einer Live-DVD erhält man ein sinnvoll vorkonfiguriertes und garantiert sauberes System ohne Trojaner. Da man keine Updates einspielen kann, sollte man regelmäßig eine aktuelle Version des ISO-Images von der Webseite herunterladen.

Linux Fast alle Linux-Distributionen und einige BSD-Derivate stellen Live-DVDs bereit. textitThe LiveCD List[1] bietet eine Übersicht. Man kann diese Live-DVDs zum Kennenlernen nutzen oder für viele kleine Aufgaben, die ein sauberes System erfordern.

TAILS *The Amnesic Incognito Live System* ist die offizielle Live-DVD von Torproject.org. Der gesamte Datenverkehr ins Internet wird in der Standardkonfiguration durch Tor geschickt. TAILS bietet die Anonymisierungsdienste Tor und I2P. Diese Live-CD kann nur mit Intel i686 Computern genutzt werden.

Download: https://tails.boum.org/

Subgraph OS ist ein besonders gehärtetes Linux mit Grsecurity/PaX Kernel Patches. Alle Anwendungen sind per Sandbox voneinander isoliert. Tor Onion Router wird standardmäßig als Anonymisierungsdienst genutzt. Derzeit steht eine Alpha Version zum Download bereit. Das ISO-Image kann auch als Live-DVD als Alternative zu TAILS genutzt werden.

18.1 USB-Sticks als Bootmedium vorbereiten

Für TAILS wird alle 6-8 Wochen eine aktualisierte Version zum Download freigegeben. Deshalb verwende ich USB-Sticks als Boot Medium statt DVDs. Regelmäßige Aktualisierung ist (nicht nur) für sicherheitsrelevante Software ein Muss. Auch andere Live-DVDs lassen sich auf USB-Sticks leichter verwenden.

[1] https://livecdlist.com/

Windows: Mit dem *Easy Universal USB Installer* von Pendrivelinux.com kann man einfach einen bootfähigen USB-Stick aus einem Linux ISO-Image erstellen. Mit dem *YUMI Multiboot USB Creator* kann man mehrere Systeme auf den USB-Stick packen.

Abbildung 18.1: Easy Universal USB Installer

Nach dem Download ist die EXE-Datei zu starten (keine Installation nötig). Man wählt die Option *Try unlisted Linux ISO image*, das herunter geladene ISO-Image und außerdem den USB-Stick, der verwendet werden soll.

Linux: Man kann auf der Kommandozeile das Tool *dd* verwenden, um ein ISO-Image auf den USB-Stick zu schieben. Nach dem Anschließen des USB-Stick benötigt man die die Device Kennung, die man Quick-and-Dirthy mit dem Kommando *ls* ermitteln kann. Üblicherweise ist der zuletzt angeschlossene USB-Stick das letzte Device in der Liste:

```
> ls /dev/sd?
/dev/sda /dev/sdb /dev/sdc
```

Dann schiebt man mit dem Tool *dd* das herunter geladenen ISO-Image auf den USB-Stick. Dabei werden alle(!) Daten und Partitionen auf dem Stick gelöscht.

```
> sudo dd if=debian-live.iso of=/dev/sdc
```

Wenn man eine Fortschrittsanzeige für den Kopiervorgang sehen will, dann kann man das Tool *buffer* verwenden:

```
> dd if=debian-live.iso | buffer -s 64k -S 10m >/dev/sdc
```

Man kann diese Methode auch in den Linux Live-DVDs nutzen, wenn man zwei USB-Sticks im Wechsel verwendet.

Für **TAILS** gibt es neben den generischen Methoden einen eigenen Installer. Unter Ubuntu 15.10+ kann man den TAILS-Installer aus einem PPA-Repository installieren:

```
> sudo add-apt-repository ppa:tails-team/tails-installer
> sudo apt update
> sudo apt install tails-installer
```

Der Installer kann TAILS auf einen neuen USB-Stick installieren oder einen bereits vorhandenen Stick mit mindesttens Version 2.0 aktualisieren.

18.2 BIOS-Einstellungen für Win8+ Rechner

TAILS und Debian Live-DVDs unterstützen kein Secure Boot. Um diese Live-DVDs mit modernen Windows 8+ kompatiblen Rechnern zu nutzen, sind Anpassungen an den BIOS-Einstellungen nötig. Sonst erhält man beim Booten des Live-Systems den Fehler:

```
Image Authorization Fail
System can not boot this device due to Security Violation.
```

Wie man die BIOS-Einstellungen öffnet, ist von Rechner zu Rechner unterschiedlich. Üblicherweise muss man in den ersten 1-2 Sekunden beim Booten des Rechners die Taste F1, F2 oder ENTF drücken. Mein Laptop hat eine extra Taste dafür. Das Handbuch zur Hardware liefert konkrete Antworten.

In der Sektion *Boot* in den BIOS-Einstellungen muss man die Option *Secure Boot* deaktivieren. Bei einigen Computern versteckt sich diese Option hinter *OS Selection* und man muss *WIN 7/others OS* wählen.
Außerdem sollte man *PXE-Boot* deaktivieren (siehe: DHCP Privacy).

Zur Vereinfachung in der täglichen Nutzung kann man die Bootreihenfolge im BIOS ändern. Standardmäßig bootet der Computer das OS vom DVD-Laufwerk oder der ersten Festplatte. Man kann den USB-Stick als erstes Boot Medium setzen. Dann bootet das installlierte OS nur, wenn der USB-Stick nicht angesteckt ist.

Alternativ kann man das beim Starten des Rechners das *BIOS Boot Select Menü* aufrufen (bei PCs üblicherweise mit den Tasten F8, F10 oder F12, bei Macs die ALT-Taste gedrückt halten), wenn man den USB-Stick nutzen will. Das Handbuch zur Hardware liefert wieder konkrete Antworten.

Kapitel 19

Smartphones

> *Wenn mir früher jemand gesagt hätte, ich würde freiwillig eine Wanze mit mir herum tragen und sie auch noch selbst aufladen, hätte ich laut gelacht. Heute habe ich ein Smartphone.*

Ob ich ein Smartphone nutze, werde ich manchmal gefragt. Gegenfrage: Braucht man das Ding wirklich oder ist es nur ein nettes Lifestyle Gadget? Für den Berliner Philosophen und Medientheoretiker Byung-Chul Han sind Smartphones das wesentliche Element zur Kontrolle der Bevölkerung im Zeitalter der Psychomacht:

> *Jede Herrschaftstechnik bringt eigene Devotionalien hervor, die zur Unterwerfung eingesetzt werden. Sie materialisieren und stabilisieren die Herrschaft ... Das Smartphone ist eine digitale Devotionalie, ja die Devotionalie des Digitalen überhaupt. Es funktioniert wie der Rosenkranz. Beide dienen der Selbstprüfung und Selbstkontrolle. Like ist das digitale Amen. Das Smartphone ist nicht nur ein effizienter Überwachungsapparat, sondern auch ein mobiler Beichtstuhl. Facebook ist die Kirche, die globale Synagoge.*

Mit der zunehmenden Verbreitung von Smartphones entstehen neue Gefahren für die Privatsphäre, die deutlich über die Gefahren durch datensammelnde Webseiten beim Surfen oder E-Mail scannen bei Mail Providern wie Google hinaus gehen. Da wir die handliche Wanze immer mit uns umhertragen und unterwegs nutzen, ist es möglich, komplexe Bewegungsprofile zu erstellen und uns bei Bedarf zu lokalisieren. Greg Skibiski beschreibt im Interview mit Technology Review seine Vision von einer Zukunft mit breiter Auswertung der via Smartphone gesammelten Daten wie folgt:

> *Es entsteht ein fast vollständiges Modell. Mit der Beobachtung der Signale kann man ganze Firmen, ganze Städte, eine ganze Gesellschaft röntgen.*

Man sollte sich darüber im Klaren sein, dass es gegen die Lokalisierung und Beobachtung von Bewegungsprofilen keinen technischen Schutz gibt.

19.1 Kommerzielle Datensammlungen

Die Auswertung der Standortdaten schafft einen neuen Markt für Werbung, der den bisherigen Markt für personenbezogene Werbung im Internet weit übertreffen soll. Bei den damit möglichen Gewinnen wundert es nicht, dass viele Teilnehmer aggressiv dabei sind, Daten zu sammeln:

- In Apples Datenschutzbestimmungen für das iPhone räumt der Konzern sich das Recht ein, den Standort des Nutzers laufend an Apple zu senden. Apple wird diese Daten Dritten zur Verfügung stellen. Für diese Datensammlungen wurde Apple mit dem BigBrother Award 2011 geehrt.

  Seit iOS Version 8 übertragen Apples Mobilgeräte automatisch die Liste der Telefonanrufe an Apple-Server (Telefonnummer, Datum/Uhrzeit, Dauer), sobald ein iCloud-Konto eingerichtet wurde. Die Datenspeicherung kann man nur verhindern, wenn man das iCloud Drive komplett abschaltet.

  Mit iOS Version 10 hat Apple diese Datenspeicherung ausgeweitet und überträgt die Metadaten der Kommunikation von allen Apps in die Apple Cloud, die mit CallKit-Unterstützung eingehende Anrufe auf dem Lockscreen anzeigen. Das betrifft neben Telefonie und SMS auch iMessage, WhatsApp, Skype und verschlüsselten VoIP Telefonate des Messengers Signal.

  Die Kommunikationsdaten werden für 4 Monate im iCloud-Konto des Benutzers gespeichert und können dort ggf. von Behörden abgegriffen und für die Kommunikationsanalyse genutzt werden. Die Firma Elcomsoft bietet Geheimdiensten die nötigen Tools, um diese Daten zu erschließen.

- Auch Googles Android Smartphones übertragen seit Version 6 (April 2016) die gesamte Call History (Telefonnummer, Datum/Uhrzeit, Dauer) in die Cloud. Auch diese Daten können gleichfalls mit den Tools der Firma Elcomsoft von Geheimdiensten und Strafverfolgung genutzt werden.

  Ich bin immer wieder verwundert, wenn Leute seit 20 Jahren gegen die gesetzliche Verpflichtung zur Vorratsdatenspeicherung (bzw. Mindestspeicherpflicht) kämpfen und bei ihren Lieblings-Lifestyle-Gadgets keine Probleme damit haben, wenn Apple oder Google die Kommunikationsdaten freiwillig auf Vorrat sammeln und Behörden zur Verfügung stellen.

- Mit der Software Carrier IQ, die auf über 140 Mio. Android Handys und auf einigen Apples iPhone installiert war, sammelten verschiedene Mobil Provider Informationen über die Nutzer. Die Software konnte nicht auf normalen Weg durch den Nutzer deinstalliert werden.

- Tausende Apps sammeln überflüssigerweise Standortdaten der Nutzer und übertragen sie an die Entwickler der Apps. Der ehem. Bundesdatenschutzbeauftragte erwähnt beispielsweise eine App, die das Smartphone

zur Taschenlampe macht und dabei den Standort an den Entwickler der App sendet. Einige Spiele der Hersteller iApps7 Inc, Ogre Games und redmicapps gehen in ihrer Sammelwut so weit, dass sie von Symantec als Malware eingestuft werden. Die Spiele-Apps fordern folgende Rechte um Werbung einzublenden:

  - ungefährer (netzwerkbasierter) Standort
  - genauer (GPS-)Standort
  - uneingeschränkter Internetzugriff
  - Browserverlauf und Lesezeichen lesen
  - Browserverlauf und Lesezeichen erstellen
  - Telefonstatus lesen und identifizieren
  - Automatisch nach dem Booten starten

  Auch Spiele von Disney verlangen sehr weitreichende Freigaben, so dass sie nur als Spionage-Tools bezeichnet werden können.

- Einige Apps beschränken sich nicht auf die Übertragung der Standortdaten und Einblendung von Werbung. Die folgenden Apps haben auch das Adressbuch der Nutzer ausgelesen und ohne Freigabe durch den Nutzer an den Service-Betreiber gesendet:

  - die Social Networks *Facebook*, *Twitter* und *Path*
  - die Location Dienste *Foursquare, Hipster* und *Foodspotting*
  - die Fotosharing App *Instagram*

  Besonders brisant wird diese Datensammlung, wenn Twitter alle Daten von Wikileaks Unterstützern an die US-Behörden herausgeben muss.

- Die App von Facebook fordert außerdem folgende Rechte:

  - Lesender Zugriff auf alle SMS und MMS
  - Zugriff auf Kalendertermine sowie vertrauliche Informationen
  - ohne das Wissen der Eigentümer Kalendertermine hinzufügen oder ändern
  - E-Mails an Gäste senden

  Ein Entwickler von Facebook versicherte, dass man diese Rechte nie voll ausnutzen wird. Die Facebook-App braucht diese Rechte nur für die Authentifizierung und um einen Kalender-Feed anzulegen. Ich bin mir ganz sicher: *Niemand hat vor...* Aber wer würde einem Mitglied der PRISM-Gruppe diese Rechte einräumen?

- Die Security-Suites von Avira, Bitdefender und AVG werben mit einer einfachen Lokalisierung des Smartphone bei Diebstahl. Dafür werden die Standortdaten ständig an die Firmen übertragen, auch wenn man den Diebstahlschutz deaktiviert hat.

19.2 Überwachung

Auch Strafverfolgungsbehörden und Geheimdienste nutzen die neuen Möglichkeiten zur *Durchleuchtung der Gesellschaft*:

- Die NSA sammelt täglich rund 5 Milliarden Standortdaten von Mobiltelefonen weltweit im Rahmen des Programms STORMBREW. Nahezu jeder Handynutzer ist betroffen. Das Analyse-Programm *Co-Traveler* sucht anhand der Standortdaten nach Verbindungen zu Zielpersonen. Wer sich zufällig mehrmals am gleichen Ort wie eine Zielperson aufgehalten hat oder zufällig im gleichen Zug saß, kann auch als Unschuldiger ins Netzwerk der Spionage geraten. Außerdem wird nach Verhaltensmustern gesucht, die auf ein erhöhtes Sicherheitsbewusstsein hindeuten.

- NSA/GCHQ sammeln täglich fast 200 Millionen SMS mit dem Programm DISHFIRE. Anhand der Datensammlung werden Kontaktbeziehungen (Identifizierung neuer Zielpersonen), Reisedaten, Finanztransfers (Konto- und Kreditkartennummern) u.a.m. analysiert.

- Das FBI nutzt das Tracking von Smartphones seit mehreren Jahren, wie Danger Room berichtete. Muslimische Communities werden systematisch analysiert, ohne dass die Personen im Verdacht stehen, eine Straftat begangen zu haben. [1].

- Im Iran werden mit Hilfe der Funkzellenauswertung die Teilnehmer von Demonstrationen in Echtzeit ermittelt. Die Technik dafür wird von westlichen Unternehmen entwickelt, beispielsweise von Siemens/Nokia und Ericsson. Nachdem die Unterstützung von Siemens/Nokia für die Überwachung bekannt wurde und ein Boykottaufruf zu mehr als 50% Umsatzeinbruch im Iran führte, wurde die Überwachungstechnik bei Siemens/Nokia in eine Tochtergesellschaft ausgelagert: Trovicor. Zu den Kunden von Trovicor zählen auch Bahrain, Katar u.ä. Diktaturen in Middle East.

- In der Ukraine wurden die Geofenching Daten von Handys bereits im Jan. 2014 zur Einschüchterung von Demonstranten genutzt. Teilnehmer einer Demonstration gegen den damals amtierenden Präsidenten bekamen eine SMS mit dem Inhalt:[2]

  > *Sehr geehrter Kunde, sie sind als Teilnehmer eines Aufruhrs registriert.*

Auch in Deutschland wird die Lokalisierung von Handys und Smartphones mittels Funkzellenauswertung zur Gewinnung von Informationen über politische Aktivisten genutzt:

- Die flächendeckende Auswertung von Handydaten im Rahmen der Demonstration GEGEN den (ehemals) größten Nazi-Aufmarsch in Europa in Dresden im Februar 2011 hat erstes Aufsehen erregt. Obwohl die Aktion von Gerichten als illegal erklärt wurde, werden die gesammelten

[1] http://www.wired.com/dangerroom/2011/10/fbi-geomaps-muslims/
[2] https://heise.de/-2095284

Daten nicht gelöscht und weiterhin für die Generierung von Verdachtsmomenten genutzt.[3]

- Seit 2005 wird diese Methode der Überwachung auch gegen politische Aktivisten eingesetzt. So wurden beispielsweise die Aktivisten der Anti-G8 Proteste per groß angelegter Funkzellenauswertung durchleuchtet.[4] Die Überwachung Handys der Aktivisten begann bereits zwei Jahre vor dem G8-Gipfel in Heiligendamm.

- Die breite Funkzellenauswertung in Berlin zur Aufklärung von Sachbeschädigungen wird als gängige Ermittlungsmethode beschrieben. Auf Anfrage musste die Polizei zugeben, dass diese Methode bisher NULL Erfolge gebracht hat.

- Die Nutzung der Stillen SMS zur Lokalisierung von Personen boomt gerade beim Verfassungschutz:

  - 1. Halbjahr 2013: 28.500 Stille SMS versendet
  - 1. Halbjahr 2014: 53.000 Stille SMS versendet
  - 2. Halbjahr 2014: 142.000 Stille SMS versendet

  Gleichzeitig stagniert die Nutzung der Stillen SMS bei Strafverfolgern (Polizei, BKA usw.) oder geht zurück. Man kann jetzt darüber spekulieren, was die Gründe für diese Aktivitäten des Verfassungsschutz sind.

- Die Bundeswehr entwickelt zusammen mit Airbus Group das Spionagesystem ISIS. Es soll an Bord einer Drohne die Überwachung von Mobilkommunikation aus der Luft ermöglichen. Wenn die Drohne über dem Gebiet Kassel, Gotha, Fulda oder Suhl kreist, könnte man mit ISIS das gesamte Gebiet der BRD überwachen.

Die Nutzung des Systems gegen Protestler wird ausdrücklich beworben:

> *Bei Protestcamps, Besetzungen u. ä. werden üblicherweise in größeren Umfang lizenzfreie Handfunkgeräte, Wi-Fi-Knoten, Schnurlostelefone und in geringerem Umfang auch Satellitentelefone eingesetzt. Üblicherweise werden diese Funksysteme von Gruppen oder*

[3] https://www.heise.de/tp/artikel/34/34973/1.html
[4] https://www.heise.de/tp/artikel/35/35043/1.html

> *Menschen mit hohem Organisationsgrad verwendet, die sich nicht auf das Funktionieren der überlasteten oder örtlich nicht verfügbaren Mobilfunknetze verlassen wollen. Der Inhalt dieser Funkverbindungen ist demzufolge aus Sicht eines Abhörers oft hochwertig, weil er Zugang zu strategischen Informationen verspricht. Für die Lokalisierung, Identifizierung und Aufzeichnung aller dieser Funksysteme ist ISIS hervorragend geeignet.*

Die Aufgaben von ISIS kann man kurz zusammenfassen: Information, Spionage, Überwachung, Identifizierung. Das System soll aus den verarbeiteten Daten die Sprecher identifizieren können und mehrere tausend Mobilfunkgeräte gleichzeitig lokalisieren und verfolgen.

Aktivierung als Abhörwanze

Dass Strafverfolger und Geheimdienste ein Handy/Smartphone remote als Abhörwanze aktivieren können, ist seit 2006 bekannt. Das FBI nutzte damals die Handys der Mafiabosse Ardito und Peluso remote zur akustischen Raumüberwachung, um Beweise zu sammeln[5]. Bereits 2007 hat das BSI deshalb empfohlen, bei Gesprächen mit sensiblen Inhalten keine Handys mitzuführen.

> *Aus Sicht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die effektivste Schutzmaßnahme ein Vermeiden des Mitführens von Handys bei Gesprächen mit sensitivem Inhalt, die Detektion jedweder Mobilfunkaktivität im Raum durch den vom BSI entwickelten Mobilfunkdetektor MDS sowie das Deaktivieren sämtlicher drahtloser Schnittstellen von Mobilfunkgeräten.*

19.3 Stille SMS ind IMSI-Catcher erkennen

Die App **Android-IMSI-Catcher-Detector** (AIMSICD) tut, was der Name sagt. Sie ist auf allen Androids einsetzbar und erfordert kein Rooten des Smartphones. Die Entwickler setzen den Open Source Gedanken konsequent um. Die App ist nicht(!) im Google PlayStore verfügbar sondern im F-Droid Store, der nur Open Source Projekte anbietet.

Die App **SnoopSnitch** von SRLabs steht seit Januar 2015 für Android im F-droid Store und im PlayStore bereit. Die App erkennt ISMI-Catcher und erkennt außerdem, ob jemand die Gespräche belauscht und mit einem SS7-Exploit die Verschlüsselung gehackt hat. Für die Installation ist ein Rooten des Smartphone nötig. Die App funktioniert nur, wenn das Smartphone einen Qualcomm Chipsatz hat.

Die App **Darshak** von R. Borgaonka (SecT, TU Berlin) kann Alarm auslösen, wenn der Standort des Smartphone mit sogenannten *Stillen SMS* getrackt wird, und kann außerdem die Sicherheitseinstellungen der Funkzelle sichtbar machen, um den Einsatz eines IMSI-Catchers zu erkennen. Die App steht auf Github zum Download bereit.[6] Sie ist derzeit nur auf dem Samsung Galaxy S3

[5] http://news.cnet.com/2100-1029-6140191.html
[6] https://github.com/darshakframework/darshak

einsetzbar und erfordert ein Rooten des Smartphone. Die Installation ist auf der Webseite beschrieben.

Das **GSMK CryptoPhone** hat einen ganz gut funktionierenden IMSI-Catcher-Detector onBoard. Mit diesem Detector wurden in Washington DC in der Umgebung des White House und US Capitol sowie in der Nähe von Botschaften 18 IMSI-Catcher aufgespürt [7].

> *I would bet money that there are governments that are spying in DC.* (C. Soghoian, ACLU)

Washington DC ist kein Einzelfall. Auch in Oslo wurden IMSI-Catcher im Regierungsviertel gefunden. Leider mussten die Journalister einer Zeitung mit einem GSMK CryptoPhone erst darauf aufmerksam machen. Die norwegische Spionageabwehr ist genauso verschlafen wie in Berlin.[8]

> *Die gefundenen Geräte seien nicht auf dem freien Markt erhältlich, sie seien sehr ausgereift und teuer. Nur Organisationen mit großen Ressourcen, etwa ausländische Geheimdienste, seien zu einer solchen Überwachung in der Lage.*

In Sicherheitskreisen vermutet man, das die IMSI-Catcher in den Regierungsvierteln in erster Linie der Beobachtung dienen, wer in den verschiedenen Einrichtungen ein- und ausgeht. Das Abhören von SMS und Telefonaten ist vermutlich eher nebensächlich. Das Smartphone ist eine Trackingwanze, die wir freiwillig mit uns umhertragen!

19.4 WLAN ausschalten, wenn nicht genutzt

Alle Smartphones (und Laptops!) haben ein WLAN Modul. Es ist bequem, wenn man nach Hause kommt oder wenn das Smartphone am Arbeitsplatz automatisch das WLAN nutzt statt der teuren Datenverbindungen des Mobilfunk Providers.

Wenn man mit aktiviertem WLAN Modul und automatischem Login für die bevorzugte WLANs unterwegs ist, dann sendet das Smartphone oder der Laptop regelmäßig aktive Probes, um die Umgebung nach den bevorzugten WALNs zu scannen. Dabei wird neben der weltweit eindeutigen MAC Adresse auch eine Liste der SSIDs der bevorzugten WLANs gesendet, mit denen sich das Smartphone automatisch verbinden würde (Prefered Network List, PNL). Diese Liste liefert Informationen über Orte, an denen sicher der Besitzer des Smartphones bevorzugt aufhält. (Home, Office...)

Mit geringem technischen Aufwand kann man diese Daten der aktiven WLAN Probes zum Tracking und für Angriffe nutzen:

1. Auf der re:publica 2013 wurde ein kostenfreies WLAN bereitgestellt. Dieses WLAN verfolgte alle WLAN-fähigen Geräte (Laptops und Smartphones) der Besucher, unabhängig davon, ob die Geräte das WLAN nutzten

[7] http://rt.com/usa/189116-washington-dc-spying-phone
[8] http://www.zeit.de/digital/datenschutz/2014-12/norwegen-spionage-oslo

oder nicht. Das Projekt *re:log - Besucherstromanalyse per re:publica W-LAN* visualisiert die Daten.[9]

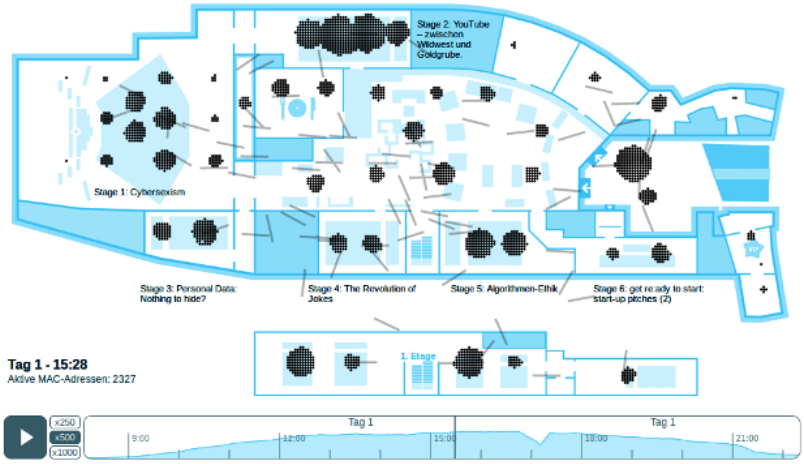


Abbildung 19.1: WLAN Tracking auf der re:publica 2013

2. Forscher der Università di Roma sind mit der Studie *Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes*[10] einen Schritt weiter gegangen. Sie haben gezeigt, dass man die aktiven WLAN Probes für eine soziale Analyse der Crowd nutzen kann. Crowd steht dabei für eine Ansammlung von Personen (Teilnehmer von Veranstaltungen oder Demonstrationen, Bordell Besucher .... usw.).

3. Die Security Firma Sensepost ging noch einen Schritt weiter. Auf der Blackhat Asia 2014 wurde die *Drohne Snoopy*[11] vorgestellt. Diese Drohne wertet die Probes der WLAN Module aus und simuliert dann die SSID eines bevorzugten WLANs des Smartphones. Das Smartphone meldet sich automatisch bei der Drohne an. Der Internet Traffic läuft über die Drohne und kann dort analysiert und modifiziert werden. Es wurde auf der Konferenz demonstriert, wie *Snoopy* Login Credentials von PayPal, Yahoo usw. abreifen konnte, Name und Wohnort der Nutzer ermitteln konnte und die Smartphones über einen längeren Zeitraum tracken konnte. Auf Githup steht der Source Code für Snoopy, Server und Webinterface für eigene Experimente zum Download bereit.

4. Android Smartphones kann ein Angreifer durch einen Fehler in der Funktion WiFi Direct kompromittieren. Dabei stellt ein Angreifer einen virtuellen Accesspoint mit einer bösartigen SSID auf. Damit kann er verwundbare System in Funkreichweite lahm zu legen, Speicherinhalte auszulesen und potenziell sogar Schadcode zur Ausführung zu bringen. Das Problem betrifft auch Linux auf dem PC oder Laptop. Solange der Fehler nicht behoben wurde, können Linuxer in der Datei

[9] http://apps.opendatacity.de/relog/
[10] http://conferences.sigcomm.org/imc/2013/papers/imc148-barberaSP106.pdf
[11] http://www.sensepost.com/blog/7557.html

/etc/wpa_supplicant/wpa_supplicant.conf folgende Option als Schutz gegen diesen Angriff aktivieren:

```
p2p_disabled=1
```

Es gibt bereits erste praktische Ansätze der Werbeindustrie, um die WLAN Probes der Smartphones zum Schnüffeln zu nutzen:

- Die Werbefirma Renew stellte zu den Olympischen Spielen 2012 in London 200 Abfallbehälter auf, die mit einem integrierten WLAN Access Point die Fußgänger anhand der MAC Adressen der Smartphones verfolgten. Innerhalb einer Woche wurde über 4 Mio. Geräte auf dem Weg durch die Londoner City verfolgt.[12]

  We will cookie the street. (K. Memari, chief executive of Renew)

- **Ins Netz gegangen** (Pressemitteilung der BVG, PDF)[13]: Die Berliner Verkehrsbetriebe werden in Zusammenarbeit mit HOTSPLOTS auf den U-Bahnhöfen kostenfreien Wi-Fi zur Verfügung stellen. Bis Ende 2016 sollen 76 U-Bahnhöfe mit den Access Points ausgestattet werden. Die Bahnhöfe wurden so gewählt, das rechnerisch 2/3 der täglich 1,5 Mio U-Bahn-Kunden erfasst werden können. Außerdem wird mit kostenfreiem WLAN auf den Buslinien 200 und 204 experimentiert.

  Die Nutzung ist ganz einfach. Wenn man beim Warten auf die U-Bahn noch schnell mal…wählt man das *BVG Wi-Fi* und ruft eine Webseite auf. Nachdem man die Nutzungsbedingungen bestätigt und die erste Werbeseite gesehen hat, kann man kostenfrei Surfen usw. Es wird kein Name und E-Mail Adresse abgefragt.

  Zukünftig meldet sich das Smartphone bei jedem Ein. und Aussteigen und bei jeder Durchfahrt durch den Bahnhof automatisch bei dem BVG Access Point an. In den Nutzungsbedingungen ganz unten (runterscrollen) findet man die Daten, die bei jedem (automatischen) Connect gespeichert werden:

  - die eindeutige MAC-Adresse des Gerätes
  - die zugewiesene IP-Adresse
  - Zeitstempel des Login und Logout

  Die Daten werden gem. TKG und gemäß Vorratsdatenspeicherung (neudeutsch: Mindestspeicherfristen) gespeichert. Außerdem werden sie von HOTSPLOTS ausgewertet und der BVG für statistische Auswertungen zur Verfügung gestellt. Diese Daten ermöglichen eine Verfolgung von Bewegungen in der realen Welt, wie es anhand der Besucherstöme auf der republica 2013 demonstriert wurde.

[12] http://rt.com/news/trash-bin-surveillance-wifi-402/
[13] http://unternehmen.bvg.de/de/index.php?section=downloads&cmd=180&download=2070

HOTSPLOTS investiert 4,9 Mio. Euro in das Projekt. Der Berliner gibt 190.000 Euro dazu. Die Investitionen müssen sich für den Investor irgendwie amortisieren. Das Projekt soll vor allem durch die Werbung finanziert werden, die auf dem Bildschirm erscheint, bevor der Internetzugang freigegeben wird.

- Die Firma AdNear experimentiert mit Drohen, welche die Wi-Fi und Baseband Signale der Smartphones auswerten. Anhand der MAC Adresse der WLAN Module der Smartphones werden die Bewegungen der Nutzer verfolgt.[14]

  > *Today we started initial tests with drones to collect data. And the results have been fantastic! Besides, this turns out to be the most efficient mode.*

Schlussfolgerung: WLAN abschalten, wenn man es nicht braucht.

19.5 WhatsApp Alternativen

Die Übernahme von WhatsApp durch Facebook zeigt, dass es einfach Sch.... ist, sich das gesamte Adressbuch mit allen Kontakten klauen zu lassen. Irgendwann landet es in den großen Datensammlungen von Google, Microsoft, Facebook oder Yahoo!, die alle als PRISM-Partner der NSA gelistet sind.

Das das FBI die Whatsapp Kommunikation belauschen konnte und die Daten an befreundete Geheimdienste weitergibt, überrascht mich nicht. Für den BND und Verfassungsschutz sind diese Daten wahrscheinlich eine Bezahlung für ihre breitwillige Kooperation.[15]

Anforderungen an einen guten Messenger

Unter Berücksichtigung des Crypto War 3.0 ergeben sich für mich folgende Anforderungen an ein guten Messenger Dienst:

1. Sichere Verschlüsselung nach dem aktuellen Stand der Technik, die durch unabhängige Experten evaluiert werden kann.

   - *Forward Secrecy* für die Ende-zu-Ende Verschlüsselung, damit die Geheimdienste bei Kompromittierung des Schlüssels nicht den gesamten, gespeicherten Datenverkehr entschlüsseln können.
   - Sichere Transportverschlüsselung (SSL/TLS) für die notwendige Kommunikation der Apps mit den Servern.
   - Prüfung der Crypto sollte durch unabhängige Experten möglich sein.

[14] https://adnear.com/february2015/experimenting-with-drones-for-data-collection.php
[15] https://heise.de/-2687028

2. Der Account sollte frei wählbar und nicht an eine Telefonnummer gebunden sein. Telefonnummern sind im Gegensatz zu E-Mail Adressen ein eindeutiges Identifizierungsmerkmal und nicht so einfach austauschbar wie (Wegwerf-) E-Mail Adressen. Das ermöglicht die Verknüpfung verschiedener Accounts bei unterschiedlichen Diensten und die Zuordnung zu einer Person.
3. Keine unerwünschten Uploads von Daten ohne ausdrückliche Bestätigung durch den Nutzer (kein Adressbuch Upload oder ähnliches).
4. Google-freie Installation (z.B. via F-Droid) sollte möglich sein.
5. Die Infrastruktur sollte dezentral verteilt sein und nicht von einem einzelnen Betreiber kontrolliert werden. Das verhindert, dass ein einzelner Provider alle Kommunikationsbeziehungen kennt. Außerdem kann ein dezentrale Infrastruktur nur schwer von Regierungen durch Gesetze kompromittiert werden, um Geheimdiensten die anlasslose Überwachung zu ermöglichen wie z.B. mit BlackBerry in Indien und Kanada, Skype allgm. oder der Gesetzentwurf zu verpflichtenden Backdoor für alle Messenger in Russland.
6. Die Server Komponente sollte ebenfalls verfügbar sein (nicht unbedingt kostenlos), damit man einen eigenen Server unabhägig vom Entwickler aufsetzen kann, um Kompromittierung des Dienstes zu erschwerden.
7. Kein Vendor-Lockin: Um zukünftig nicht bei einem Anbieter gefangen zu bleiben, der heute vielleicht ganz nett ist aber zukünftig auf der Welle des Erfolgs seine Strategie und Verhalten ändern könnte, sollten offene Protokolle genutzt werden, die eine federale Struktur der Server erlauben.

Diskussion der Alternativen

Es gibt mindestens 70 Alternativen zu Whatsapp. Die folgende Liste ist nur eine kleine Auswahl populärer Messaging Dienste.

TextSecure, Signal 2.0 von WhisperSystems wurden von Security-Experten aufgrund der guten Ende-zu-Ende Verschlüsselung empfohlen. Die von M. Marlspike entwickelte Ende-zu-Ende Verschlüsselung für TextSecure ist inzwischen der Quasi-Standard für KryptoMessenger.

> *I'm not really into advertising for stuff here but the recent update of TextSecure made a gigantic impression on me. The application works well, is uber user friendly, and looks just great. They further added IM like functionality (using IP rather then SMS).* (Collin R. Mulliner)
>
> *For the record - @moxie writes crypto software that blinds the #NSA & #GCHQ. He is their nightmare. Usable crypto developer with a backbone!* (Jakob Appelbaum)

Signal kann Google-frei genutzt werden. Dafür muss man die App von der Download Webseite herunterladen und lokal installieren. Die Google Cloud Services (GCM) werden in dieser Version nicht genutzt.[16]

[16] https://signal.org/android/apk

Es gibt aber auch Nachteile:

- Die Telefonnummern aus dem Adressbuch werden bei der Installation als Hash ungefragt hochgeladen. In einem Blogartikel erklärt M. Marlspike, dass die Hashes der Telefonnummern nur geringen Schutz bieten.[17]
- Die Telefonnummer wird als Account Kenung verwendet.
- Die Server der Infrastrukktur stehen alle in den USA.

Threema und Hoccer verschlüsseln standardmäßig alle Chats. Sie sind privacy-freundlich und verzichten auf den Upload des Adressbuches der Nutzer (bei Threma optional). Beide Messenger verwenden im Gegensatz zu WhisperSystems und allen anderen Messengern nicht die eigene Telefonnummer als Kennung, sondern eine ID, die unabhängig von anderen Daten ist. Das ist ein weiteres Privacyfeature.

Die Software ist nicht Open Source und die Betreiber kontrollieren neben der Softwareentwicklung auch die Infrastruktur vollständig. Sie könnten zukünftig wie Skype 2004 zur Implementierung von Backdoors für staatliche Behörden verpflichtet werden. Im August 2016 hatten die Innenminister Thomas de Maizière (CDU) und Bernard Cazeneuve die Forderung bekräftigt, das es für Behörden möglich sein muss, die Kommunikation von KryptoMessengern zu entschlüsseln (Crypto War 3.0). Außerdem verfügen die Provider über sämtliche Kommunikationsdaten (wer mit wem kommuniziert) und müssen diese Daten im Rahmen der Vorratsdatenspeicherung protokollieren.

Telegram, Google Allo, FB Messenger Alle drei Messenger bieten inzwischen eine optionale Ende-zu-Ende Verschlüsselung, die man für jeden privaten Chat einzeln aktivieren muss. Der Upload des kompletten Adressbuches ist Standard und kann nicht unterbunden werden, selbst wenn man die Messenger nur für wenige, einzelne Kontakte nutzen möchte. (Nicht empfehlenswert.)

Telegram bietet eine Web-App für den Desktop-PC. Diese Web-App gibt Behörden die Möglichkeit, die Kommunikation auch dann zu belauschen, auch die Ende-Ende-Ende Verschlüsselung aktiviert wurde. Das Team von Prof. Fedderath demonstrierte es: die Behörden müssen die Telefonnummer des zu belauschenden Account eingeben und dann die SMS zur Authorisierung des Zugriff auf die Kommunikation abfangen. Dann kann auch die Ende-zu-Ende verschlüsselte Kommunikation mitgelesen werden.[18]

Um diesen Angriff zu verhindern, sollte man die zweistufige Bestätigung aktivieren und so ein zusätzliches Passwort zum Aktivieren von neuen Geräten festlegen. Nur die Kenntnis der Bestätigungs-SMS reicht dann

[17] https://whispersystems.org/blog/contact-discovery/
[18] https://www.youtube.com/watch?v=wBaj0LxcnY8

nicht mehr aus, um mit der Telegram Web-App die verschlüsselte Kommunikation mitzulesen.

iMessage von Apple bietet eine kaputte Ende-zu-Ende Verschlüsselung ohne Forward Secrecy, die Apple PR-mäßig laut schreiend vermarktet hat. Auf der Usenix Conference im Aug. 2016 wurde ein erfolgreicher Angriff auf die Verschlüsselung publiziert: *Dancing on the Lip of the Volcano*[19]. Die Forscher empfehlen dringend, dass Apple die eigene Verschlüsselung wegwerfen und Axolotl von M. Marlspike verwenden sollte.

Außerdem speichert iMessage Backups der Protokolle der Kommunikation unverschlüsselt in der iCloud. Auf diese Daten hat Apple Zugriff und kann sie den Behörden zur Verfügung stellen[20]. Die Speicherung der unverschlüsselten Protokolle von verschlüsselter Kommunikation ist ein schwerer Security Bug. Wenn man diese Protokolle auch noch in der Cloud des Providers speichert, dann ist die ganze Ende-zu-Ende Verschlüsselung sinnlos und muss man schon von einer Backdoor sprechen.

Tox ist eine interessante Anwendung für verschlüsseltes Chats und Telefonie. Im Gegensatz zu allen anderen Messengern arbeitet Tox serverlos, die Kommunikation läuft direkt von Client zu Client. Damit gibt es keinen Provider, der Kommunikationsprofile erstellen könnte oder zur Implementierung von Backdoors für Behörden gezwungen werden könnte. Gleichzeitig gibt es aber auch Einschränkungen in der Usability. Um einen Kontakt aufzunehmen, muss man eine 76-stellige ID über einen sicheren Kanal austauschen, z.B. bei einem persönlichen Treffen.

Außerdem verwendet Tox für die Krypto nicht die üblichen, vom NIST standartisierten Verfahren sondern kryptografische Verfahren von D.J. Bernstein. Der ECDHE Schlüsseltausch nutzt *curve25519*, statt AES wird *xsalsa20* verwendet und statt SHA256 kommt *poly1350* zum Einsatz.

Mit *Antox* (für Android) und *Antidote* (für iOS) gibt es Alpha-Versionen für Smartphones, die aber noch einige Bugs haben.

E-Mail ist das am häufigsten genutzte Medium für Textnachrichten. Als Realitätscheck ein Vergleich mit den genannten Messenger Diensten:

- E-Mails werden in der Regel unverschlüsselt gesendet. Die großen E-Mail Provider wie Google oder Microsoft lesen ungeniert mit. Auch wenn man selbst einen privacy-freundlichen E-Mail Provider nutzt, ist man nicht gegen das Mitlesen nicht geschützt, weil:

  Google has most of my emails, because it has all of yours.
- Die zusätzliche Installation und Konfiguration von OpenPGP für die Ende-zu-Ende Verschlüsselung ist kompliziert. Es gibt keine Ende-zu-Ende Verschlüsselung mit *Forward Secrecy* für E-Mails.
- Der Austausch von Schlüsseln für OpenPGP oder S/MIME muss per Hand erfolgen, es gibt keinen vertrauenswürdigen Automatismus. Außerdem müssen die Schlüssel per Hand verifiziert werden.

[19] https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garman.pdf
[20] https://heise.de/-2807703

- Die Sicherheit der Transportverschlüsselung (SSL/TLS) zwischen den Mailservern schwankt von *nicht vorhanden* bis *möglicherweise verschlüsselt, wenn keiner angreift*. Garantierte TLS-Verschlüsselung und Certificate Pinning in Form von DANE/TLSA gibt es erst in kleinen Ansätzen bei sehr wenigen Mailprovidern.

Schlussfolgerung: Trotz der Mängel haben die oben genannten Alternativen zu WhatsApp wie TextSecure, Threema oder Hoccer erhebliche Vorteile gegenüber E-Mails hinsichtlich der Verschlüsselung. Deshalb stehen Messenger im Crypto War 3.0 generell im Focus bei der Forderung nach Backdoors, während (bisher) keine Backdoors für verschlüsselte E-Mails gefordert werden.

Empfehlung für Messenger auf dem Smartphone

Wir empfehlen Jabber/XMPP. Dieser Standard bietet eine dezentrale Infrastruktur und kann nur schwer kompromittiert werden, die Software ist Open Source und mit OMEMO und OTR stehen gute Verfahren für Ende-zu-Ende Verschlüsselung zur Verfügung.

- Für Android empfehlen wir die App *Conversations*. Man kann OMEMO, OTR und OpenPGP für die Verschlüsselung nutzen und TorOnion Router (OrBot) als Anonymisierungsdienst.
- Die App *ChatSecure* für iPhones kann ebenfalls OMEMO und OTR für die Ende-zu-Ende Verschlüsselung verwenden.
- Ein neues Projekt ist *Zom*, das als Nachfolger von ChatSecure für Android und iPhone ein modernes GUI mit dem Unterbau von Conversations verbindet.[21]

19.6 Crypto-Apps

Eine Warnung: Jede kryptografische Anwendung braucht einen vertrauenswürdigen Anker. Üblicherweise geht man davon aus, dass der eigene PC oder Laptop ein derartiger vertrauenswürdiger Anker ist, über den der Nutzer die volle Kontrolle hat. Bei Smartphones kann man nicht davon ausgehen, dass der Nutzer volle Kontrolle über die installierte Software hat.

1. Mit dem Kill Switch hat Google die Möglichkeit, auf Android Handys beliebige Apps zu deinstallieren, zu installieren oder auszutauschen. Auch alternative Mods auf Basis von Android wie cyanogenmod enthalten den Kill Switch, da er nicht im Open Source Teil von Android implementiert ist. Das iPhone[22], Windows Phone[23] und Amazons Kindle[24] haben ebenfalls einen Kill Switch. Jede Crypto-Anwendung aus den Markets muss also als potentiell kompromittiert gelten. Sie kann genau

[21] hhttps://chatsecure.org/blog/chatsecure-conversations-zom/
[22] http://www.engadget.com/2008/08/07/iphone-hacker-says-the-device-calls-home-to-apple-allows-apps/
[23] https://heise.de/-1131297
[24] https://heise.de/-6887

dann versagen, wenn man den Schutz am nötigsten braucht.

Hinweis: Die App **SecDroid** deaktiviert den Killswitch auf Android Smartphones. Sie kann aus dem F-Droid Store installiert werden.

2. Jede Crypto-Anwendung benötigt gute Zufallszahlen. Der Zufallszahlengenerator der Android Java VM ist so besch.... schlecht, dass man als Angreifer nicht die Kompetenz und Rechenleistung der Crypto-City von Fort Meade braucht. Ganz gewöhnliche Hacker konnten die Schwächen der Android Implementierung im Sommer 2013 nutzen, um Geldbörsen von Bitcoin Nutzern leer zu räumen[25].

3. Smartphones sind leicht kompromittierbar:

   - Remote Code Execution ist normalerweise ein schwerer Sicherheitsfehler. Bei Android Smartphones ist es ein Feature. Apps können Code aus dem Internet nachladen, der weder von Sicherheitsscanner auf dem Smartphone noch von den Sicherheitsprüfungen in App Stores kontrolliert werden kann. Viele kostenlose Apps für Spiele nutzen diese Möglichkeit für Werbezwecke. Da die Verschlüsselung der Internetverbindungen zu den Servern nicht immer dem aktuellen Stand entspricht oder garnicht vorhanden ist, kann ein Angreifer gezielt bestimmte Smartphones mit Trojanern verseuchen, indem er den Download on-the-fly modifiziert.
   - Der Sicherheitsexperte C. Mulliner hat das *Dynamic Dalvik Instrumentation Framework for Android* entwickelt, mit dem man jegliche Kryptografie komplett aushebeln kann. In seinem Blogartikel weist C. Mulliner darauf hin, dass er zum Deployment des Frameworks nichts schreiben muss, weil für dieses Problem genügend Lösungen publiziert wurden.
   - Auch das *Xposed Framework* kann mit einem ähnlichen Trick Kryptografie komplett aushebeln oder die Privacy-Einstellungen verschärfen (je nach Intention).

Einige Crypto-Apps

Wer trotzdem ein besseres Gefühl im Bauch hat, wenn die Kommunikation verschlüsselt wird, kann folgende Apps nutzen:

- **CSipSimple** und **Redphone** sind VoIP-Softphones mit ZRTP-Verschlüsselung der Gespräche (siehe Kapitel: VoIP) und für verschlüsselte Textnachrichten.
- **Groundwire** ist ein VoIP-Softphones mit ZRTP-Verschlüsselung und OSTN-Support für das iPhone.
- **Silent Circle** ist ein komerzielles Projekt von Phil Zimmermann, dass für iPhone und Windows verschlüsselte Internettelefonie bietet.[26]

[25] https://heise.de/-1933714
[26] https://silentcircle.com

- Für das iPhone und iPad gibt es den **Onion Bowser** für im App Store. Der minimalistische Browser enthält Tor Onion Router und benötigt keine weiteren Konfigurationsschritte.

OpenPGP-Verschlüsselung

Man kann OpenPGP auch auf dem Smartphone nutzen, aber:

> *Never store your private PGP key on your mobile phone... Mobile phones are inherently insecure.* (Mike Cardwell)

Der Yubikey NEO hat eine OpenPGP Smartcard, die via NFC genutzt werden kann. Der private Schlüssel wird dabei auf dem Yubikey gespeichert und verlässt diese Umgebung nie. Die PIN zur Freigabe des Schlüssel wird zusammen mit den zu entschlüsselnden oder zu signierenden Daten via NFC an den Yubikey gesendet und das Ergebnis der Kryptooperation wird zurück an das Smartphone gegeben.

1. Auf dem Andoid Smartphone benötigt man folgende Software, die man aus dem Google Play Store oder F-Droid Store installieren kann:
   - **OpenKeychain** kümmert sich um Ver-/Entschlüsselung und die Verwaltung der Schlüssel. Seit Version 3.2 vom 06. Mai 2015 wird der Yubikey NEO via NFC als OpenPGP Smartcard unterstützt.
   - Das E-Mail Programm **K9mail** kann direkt mit OpenKeychain zusammenarbeiten und integriert Buttons zum Verschlüsseln bzw. Entschlüsseln von E-Mails in das GUI.
   - Der Jabber/XMPP Client **Conversations** kann in Kombination mit OpenKeychain die Chats mit OpenPGP verschlüsseln, der private Key liegt dabei aber auf dem Smartphone. OTR- und OMEMO-Verschlüsselung sind auch möglich.
2. Den Yubikey NEO bereitet man am einfachsten mit Enigmail auf einem PC vor (siehe: OpenPGP Smartcards). Die OpenPGP Smartcard Funktion ist freizuschalten, die PIN und Admin-PIN ist zu ändern und die Schlüssel sind zu generieren.
3. Das neu erstellte Schlüsselpaar kann man aus Enigmail in eine Datei exportieren (geheimen + öffentlichen Schlüssel!). Der geheime Schlüssel in dieser Datei enthält praktisch nur einen Verweis, welche Smartcard genutzt werden muss.
4. Diese Schlüsseldatei ist auf das Smartphone zu übertragen und in OpenKeychain zu importieren.
5. Außerdem muss man noch die öffentlichen Schlüssel der Kommunikationspartner in OpenKeychain auf dem Smartphone importieren. Diese Schlüssel kann man ebenfalls aus Enigmail exportieren, wenn sie dort vorhanden sind. Alle benötigten Schlüssel können markiert werden (STRG-Taste drücken, wenn der Schlüssel mit der Maus markiert wrid) und in eine Datei zusammen gespeichert werden. Diese Datei wird ebenfalls auf das Smartphone übertragen und in OpenKeychain importiert.

19.7 Das Hidden OS im Smartphone

In jedem Smartphone steckt neben dem End-User-Betriebssystem (Android, iOS, Windows Phone) und dem Linux Kernel ein weiteres, verstecktes Betriebssystem. Dieses Hidden OS läuft auf dem Breitband Prozessor und bearbeitet die Kommunikation mit den Mobilfunkstationen in Echtzeit. Es handelt sich dabei um ein Real-Time Betriebssystem. Der Markt wird von Qualcomm mit AMSS dominiert, die Software ist Closed Source.

Im Betrieb hat das Hidden OS die volle Kontrolle über die gesamte Hardware incl. Mikrofon und Kamera. Linux Kernel und End-User Betriebssysteme laufen als Slaves unter Kontrolle des Hidden OS.

Die implementierten Sicherheitsstandards des Hidden OS stammen aus dem vergangenen Jahrhundert. Die Daten der Mobilfunkstationen werden z.B. ungeprüft als valid übernommen. Security Analysen sind schwierig, da jede Anlalyse zuerst ein Reverse Engeniering der Closed Source Software erfordert. Trotzdem stellen Sicherheitsexperten seit Jahren immer wieder gravierende Mängel vor:

- Ralf Philipp Weinmann stellte auf der DeepSec 2010 ein Angriff auf Androids und iPhones vor, der mit mit einem nur 73 Byte Remote Code Execution Exploit eine Backdoor öffnete und das Smartphone in eine Abhörwanze verwandelte: *All Your Baseband Are Belong To Us*.[27]
- Mit den *Hexagon challenges* wurde auf der PacSec 2013 ein verbesserten Angriff auf das Hidden OS von Weinmann vorgestellt.[28]
- Forscher der TU Berlin demonstrierten auf dem *22nd USENIX Security Symposium* eine Angriff auf das Hidden OS, der nur geringe Resourcen erforderte. Mit einigen manipulierten Smartphones wurden andere Smartphones in der Umgebung kompromittiert und der Empfang von Anrufen und SMS blockiert.[29]

19.8 Blackphone

Aus dem oben Geschriebenen ergeben sich die Schlussfolgerungen, welche Verbesserungen hinsichtlich Privatsphäre für Projekte wie das Blackphone u.ä. möglich sind.

1. Das Blackphone kann durch sinnvolle Standardkonfiguration gegen kommerzielle Datensammlungen schützen. Da die Entwicklung und Produktion nicht durch Auswertung von gesammelten Daten subventioniert werden kann, ist das Blackphone deutlich teuerer als technisch gleichwertige Smartphones für den Mainstream Nutzer.
2. Da es ein mobiles Smartphone sein will, muss es einen zugelassenen Baseband Prozessor incl. Hidden OS verwenden (anderenfalls würde man

[27] http://www.securitytube.net/video/5372
[28] http://pacsec.jp/speakers.html
[29] http://phys.org/news/2013-08-firmware-tweak-block-subscriber-berlin.html

es *Laptop* oder textitNotebook nennen). Es kann daher nicht gegen staatliche Überwachung schützen.

> *Wenn die NSA hinter Ihnen her ist, wird Sie auch das Blackphone nicht schützen.* (Phil Zimmermann)

Das Blackphone Silent OS 3.0 enthält ein *Cellular Intrusion Detection System* (CIDS), das viele Angriffe auf Ebene des Baseband erkennt und den Nutzer warnt. Stille SMS zum genauen Tracking werden angezeigt, Netzwerk Downgrades sowie schwache oder deaktivierte Verschlüsselung werden ebenfalls erkannt und als Warnung angezeigt.[30]

3. Das Blackphone bietet mehrere verschlüsselte Container, die die Verschlüsselung ernsthaft umsetzen und bei Beschlagnahme des Smartphones die Daten zuverlässig schützen können. Neben den Daten werden auch installierte Apps geschützt. Die einzelnen Container sind gegeneinander isoliert und können für unterschiedliche Zwecke genutzt werden (beruflich, privat, politische Aktivitäten o.ä.).

   Es kommt schon mal vor, dass die Polizei bei einer Spontandemo 150 Menschen einkesselt und man den Kessel nur verlassen darf, wenn man sein Smartphone zwecks Auslesen aller Daten übergibt. Es ist dann aber auch schade um das schöne Smartphone, wenn die Polizei an der Verschlüsselung scheitert und die nicht knackbaren Smarthone nicht zurück geben will (ohne Anklage gegen die Besitzer).[31]

   Das Beispiel zeigt deutlich, dass Polizei und "Diensteëin immer größeres Interesse an den Daten, Adressbüchern usw. der Smartphones politischer Aktivisten entwickeln.

4. Updates für das Betriebssystem können zuverlässig und schnell geliefert werden. Außerdem kann ein App Store zur Verfügung gestellt werden, der im Gegensatz zu Google Play oder dem iPhone Store die Privatsphäre der Nutzer respektiert.

5. Da das Blackphone grundsätzlich kompatibel mit der Android Plattform bleiben will, kann man natürlich beliebige, schnüffelnde Apps aus Google Play nachinstallieren. Das Blackphone kann versuchen, die Zugriffrechte besser zu kontrollieren. Wenn der User diese Möglichkeiten aber nicht nutzt und die geforderten Rechte freigibt, um die App wie gewohnt nutzen zu können, dann ist auch das Blackphone machtlos.

[30] https://www.silentcircle.com/blog/introducing-silent-os-3-0-and-the-privacy-meter
[31] https://netzpolitik.org/2015/leipziger-polizei-mauert-nach-spontandemonstration-beschlagnahmte-150-handys-werden-nicht-herausgegeben